

COMPUTING WITH INFINITE OBJECTS: THE GRAY CODE CASE

DIETER SPREEN ^a AND ULRICH BERGER ^b

^a Department of Mathematics, University of Siegen, 57068 Siegen, Germany
e-mail address: spreen@math.uni-siegen.de

^b Department of Computer Science, Swansea University, The Computational Foundry, Swansea University Bay Campus, Fabian Way, Swansea, SA1 8EN, UK
e-mail address: u.berger@swansea.ac.uk


ABSTRACT. Infinite Gray code has been introduced by Tsuiki [Ts02] as a redundancy-free representation of the reals. In applications the signed digit representation is mostly used which has maximal redundancy. Tsuiki presented a functional program converting signed digit code into infinite Gray code. Moreover, he showed that infinite Gray code can effectively be converted into signed digit code, but the program needs to have some non-deterministic features (see also [TS05]). Berger and Tsuiki [BT21a, BT21b] reproved the result in a system of formal first-order intuitionistic logic extended by inductive and co-inductive definitions, as well as some new logical connectives capturing concurrent behaviour. The programs extracted from the proofs are exactly the ones given by Tsuiki. In order to do so, co-inductive predicates \mathbf{S} and \mathbf{G} are defined and the inclusion $\mathbf{S} \subseteq \mathbf{G}$ is derived. For the converse inclusion the new logical connectives are used to introduce a concurrent version \mathbf{S}_2 of \mathbf{S} and $\mathbf{G} \subseteq \mathbf{S}_2$ is shown. What one is looking for, however, is an equivalence proof of the involved concepts. One of the main aims of the present paper is to close the gap. A concurrent version \mathbf{G}^* of \mathbf{G} and a modification \mathbf{S}^* of \mathbf{S}_2 are presented such that $\mathbf{S}^* = \mathbf{G}^*$. A crucial tool in [BT21a] is a formulation of the Archimedean property of the real numbers as an induction principle. We introduce a concurrent version of this principle which allows us to prove that \mathbf{S}^* and \mathbf{G}^* coincide. A further central contribution is the extension of the above results to the hyperspace of non-empty compact subsets of the reals.

CONTENTS

1. Introduction	2
2. Digit Spaces	7
3. Inductive and co-inductive definitions	12
4. Extracting algorithmic content from co-inductive proofs	15

2012 ACM CCS: D.2.4.; F.4.1; I.2.2; I.2.3; I.2.4.

Key words and phrases: Computing, real numbers, compact sets, signed-digit representation, Gray code representation, iterative function systems, program extraction, logic, inductive definition, co-inductive definition, constructive mathematics.

 This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

5. Computationally motivated logical connectives	25
6. Concurrent Archimedean induction	37
7. Concurrent signed digit and Gray codes	38
8. The compact sets case	44
9. Archimedean induction for compact sets	46
10. Signed digit and Gray code for non-empty compact sets	51
11. Concurrent Gray code for non-empty compact sets	56
12. Conclusion	60
Acknowledgement	61
References	61

1. INTRODUCTION

In investigations on exact computations with continuous objects such as the real numbers, objects are usually represented by streams of finite data. This is true for theoretical studies in the Type-Two Theory of Effectivity approach (cf. e.g. [We00]) as for practical research, where prevalently the signed digit representation is used (cf. [CG06, ME07, BH08]), but also others [ES98, EH02, Ts02]. In [Be11] it is shown how to use the method of program extraction from proofs to extract certified algorithms working with the signed digit representation in a semi-constructive logic allowing inductive and co-inductive definitions. In addition to producing correct algorithms, this approach allows reasoning in a representation-free way, as in usual mathematical practice. Concrete representations of the objects needed in computations are generated automatically by the extraction procedure. A detailed description of the logic (i.e. *Intuitionistic Fixed Point Logic (IFP)*) and the realisability approach used for extracting programs can be found in [BT21a].

In order to generalise from the different finite objects used in the various stream representations, the present authors [BS16] used the abstract framework of what was coined *digit space*, i.e. a bounded complete non-empty metric space X enriched with a finite set D of contractions on X , called *digits*, that cover the space, that is

$$X = \bigcup \{ d[X] \mid d \in D \},$$

where $d[X] = \{ d(x) \mid x \in X \}$.

Digit spaces are compact and weakly hyperbolic, where the latter property means that for every infinite sequence d_0, d_1, \dots of digits the intersection $\bigcap_{n \in \mathbb{N}} d_0 \circ \dots \circ d_n[X]$ contains *at most* one point [Ed96]. Compactness on the other hand, implies that each such intersection contains *at least* a point. By this way every stream of digits denotes a uniquely determined point in X . Because of the covering property it follows conversely that each point in X has such a code.

The framework has been generalised in [Sp21]. In both papers the proof of the main results required a strengthening of the covering condition in such way that

$$X = \bigcup \{ \text{int}(d[X]) \mid d \in D \},$$

where for a subset A of X , $\text{int}(A)$ is the topological interior of A . Spaces with this property were called *well-covering*. The usual spaces occurring in applications are of this kind,

in particular the space (\mathbb{I}, SD) consisting of the real interval $\mathbb{I} \stackrel{\text{Def}}{=} [-1, 1]$ and the set $\text{SD} \stackrel{\text{Def}}{=} \{ \lambda x. (x + d)/2 \mid (d = -1 \vee d = 1) \vee d = 0 \}$ whose streams of digits are used in the *signed digit representation*.

An important example of a non-well-covering digit space is the space (\mathbb{I}, GC) with $\text{GC} \stackrel{\text{Def}}{=} \{ \lambda x. -d \cdot (x - 1)/2 \mid d = -1 \vee d = 1 \}$ leading to an extension of finite Gray code to infinite words over the alphabet $\{-1, 1\}$, by which each real number in \mathbb{I} except the dyadic rationals in $(-1, 1)$ is represented by exactly one word. Dyadic rationals are represented by two words that differ in only one place. It follows that the corresponding cell contains no information. Tsuiki [Ts02] suggested to identify both codes and to fill the cell in which they differ with the symbol \perp for ‘*unknown*’. Note that the symbol \perp is of a different kind than -1 or 1 . It is like the symbol for ‘*blank*’ on a Turing tape which can also be re-written in the course of the computation. By this way a redundancy-free representation of the interval $[-1, 1]$ is obtained, also called *infinite Gray code*.

There is, however, a price to be paid for getting rid of redundancy. Tsuiki [Ts02] proved that the computability notion for real numbers that is obtained with respect to the new representation is equivalent to the widely accepted computability notion based on the Type-Two Theory of Effectivity approach. To this end he showed that there are computable translations from streams of digits of a real number with respect to the signed digit representation into a stream representing the same number in infinite Gray code, and vice versa. As turned out, the translation of infinite Gray code into signed digit representation cannot be computed purely sequentially: one must have access not only to the head of the input stream, but also to the entry next to it, similarly when writing. To this end, the algorithm has to work non-deterministically.

The representation of elements of a digit space (X, D) by streams of digits can be characterised co-inductively. Let $\mathbb{C}_X \subseteq X$ be co-inductively defined by

$$x \in \mathbb{C}_X \stackrel{\nu}{=} (\exists d \in D)(\exists y \in \mathbb{C}_X) x = d(y),$$

that is, \mathbb{C}_X is the largest subset of X satisfying the equation (see Section 3 for the theory of inductive and co-inductive definitions). Then from a constructive proof that $x \in \mathbb{C}_X$ one can extract a stream of digits representing x . Note that from the covering property of digit spaces it follows (by co-induction) that $X \subseteq \mathbb{C}_X$. However, in general this is only true in classical logic since for an arbitrary element $x \in X$ one can usually not determine constructively a digit $d \in D$ whose image contains x . Hence, constructively, \mathbb{C}_X is normally a proper subset of X . However, if the digit space has an effective basis and is well-covering, then \mathbb{C}_X yields a representation of X that is constructively equivalent to the standard Cauchy representation. Since this is the case for the digit space (\mathbb{I}, SD) , we let $\mathbf{S} = \mathbb{C}_{(\mathbb{I}, \text{SD})}$, and obtain \mathbf{S} as the largest set of real numbers in $[-1, 1]$ that (constructively) has a signed digit representation.

The same approach does not work for infinite Gray code since, as pointed out earlier, its digit space, (\mathbb{I}, GC) , is non-well covering. Nevertheless, Berger and Tsuiki presented in [BT21a], the following co-inductive characterisation \mathbf{G} of the interval \mathbb{I} that does allow for the extraction of infinite Gray code:

$$\mathbf{G}(x) \stackrel{\nu}{=} (-1 \leq x \leq 1) \wedge \mathbf{D}(x) \wedge \mathbf{G}(\mathbf{t}(x)).$$

Here, $\mathbf{D}(x) \stackrel{\text{Def}}{=} x \neq 0 \rightarrow (x \leq 0 \vee x \geq 0)$, and \mathbf{t} is the tent function $\mathbf{t}(x) \stackrel{\text{Def}}{=} 1 - 2|x|$ which is the continuous join of the inverses of the digits in GC. Note that, if $x \neq 0$, then a realiser

of $\mathbf{D}(x)$ is a digit deciding the disjunction $x \leq 0 \vee x \geq 0$. However, in the case $x = 0$ the realiser may be undefined. This provides a logical explanation why an infinite Gray code may contain an undefined digit. In [BT21a] it is shown that that $\mathbf{S} \subseteq \mathbf{G}$ is provable in IFP and that the extracted algorithm is exactly the translation from signed digit representation into infinite Gray code given in [Ts02].

When trying to extract Tsuiki's translation in the opposite direction from a proof of $\mathbf{G} \subseteq \mathbf{S}$, one faces the obstacle that IFP, being based on traditional realisability, can only extract algorithms that are deterministic and sequential, while, as discussed above, an effective translation from infinite Gray code to the signed digit representation is necessarily non-deterministic and concurrent. To overcome this limitation of IFP, in [BT21b] an extension of IFP, *Concurrent Fixed Point Logic (CFP)*, is developed. Its main novelty is a *concurrency modality* $\Downarrow(A)$ indicating that realisers of A may be computed by two concurrent threads, where the result of the thread terminating first is taken as realiser and the other thread is discarded. More precisely, realisability of $\Downarrow(A)$ is defined using a version of McCarthy's *Amb* [MC63]:

$$\begin{aligned} c \mathbf{r} \Downarrow(A) &\stackrel{\text{Def}}{=} c = \mathbf{Amb}(a, b) \wedge \\ &\quad (a \neq \perp \vee b \neq \perp) \wedge \\ &\quad (a \neq \perp \rightarrow a \mathbf{r} A) \wedge (b \neq \perp \rightarrow b \mathbf{r} A). \end{aligned}$$

Besides solving the above translation problem, the motivation for introducing this modality is the wish to provide a constructive interpretation of the law of excluded middle

$$\frac{B \rightarrow A \quad \neg B \rightarrow A}{A} \text{ (lem)}$$

where B is a formula without computational content. The idea is that (lem) should be realised by \mathbf{Amb} , since a realiser of the conclusion should be computable by running the given realisers of the two premises in parallel. It turns out that, to make this work, it is not enough to add the concurrency modality to the conclusion: one must also modify the premises to avoid false positives. This results in the rule

$$\frac{A \upharpoonright_B \quad A \upharpoonright_{\neg B}}{\Downarrow(A)} \text{ (}\Downarrow\text{-lem)}$$

where $A \upharpoonright_B$ is a strengthening of the implication $B \rightarrow A$, called *restriction*¹, that guarantees that all its defined realisers are in fact realisers of A , independently of the truth value of B . More precisely, realisability for restriction is defined as

$$a \mathbf{r} A \upharpoonright_B \stackrel{\text{Def}}{=} (B \rightarrow a \neq \perp) \wedge (a \neq \perp \rightarrow a \mathbf{r} A).$$

whereas $a \mathbf{r} (B \rightarrow A) \stackrel{\text{Def}}{=} B \rightarrow a \mathbf{r} A$. The definitions of realisability for the concurrency modality and restriction shown above are slightly simplified; for full definitions, see Section 5.

In [BT21b] the definition of \mathbf{S} is modified by making use of the new modality for concurrency:

$$\mathbf{S}_2(x) \stackrel{\nu}{=} \Downarrow((\exists d \in \mathbf{SD}) \mathbf{II}(d, x) \wedge \mathbf{S}_2(2x - d)),$$

where $\mathbf{II}(d, x) \stackrel{\text{Def}}{=} |2x - d| \leq 1$. In terms of realisability, $\mathbf{S}_2(x)$ means that a signed digit representation of x is obtained through the concurrent computation of two threads. Now,

¹In [BT21b] the notation $A \upharpoonright_B$ is used instead of $A \upharpoonright_B$.

the inclusion $\mathbf{G} \subseteq \mathbf{S}_2$ can be derived ([BT21b], see also Theorem 7.1), and it turns out that the extracted algorithm is the one given in [Ts02].

So far, we reviewed the results in [BT21a] and [BT21b] which our work builds on. In the following we give an overview of the main new result of the present paper.

As we have seen, from the results in [BT21a] and [BT21b] it follows that $\mathbf{S} \subseteq \mathbf{G} \subseteq \mathbf{S}_2$. What one is looking for, however, is a proof of the equivalence of the involved concepts. In this paper we present a concurrent version \mathbf{G}^* of \mathbf{G} and a modification \mathbf{S}^* of \mathbf{S}_2 so that $\mathbf{S}^* = \mathbf{G}^*$. \mathbf{S}^* and \mathbf{G}^* are defined with the following iterated form of the concurrency operator (cf. Section 5.3):

$$\Downarrow^*(A) \stackrel{\mu}{=} \Downarrow^*(A \vee \Downarrow^*(A)).$$

where $\stackrel{\mu}{=}$ indicates that $\Downarrow^*(A)$ is the *least* (i.e. logically strongest) proposition satisfying the equation. A realiser of $\Downarrow^*(A)$ consists of two concurrent threads of computations, $\mathbf{Amb}(a, b)$, where each thread, if terminating, either provides a realiser of A , or else a new concurrent computation. Since the least fixed point is taken, the first alternative is guaranteed to happen, eventually.

\mathbf{S}^* is now defined like \mathbf{S}_2 , but with \Downarrow^* instead of \Downarrow (see Section 7):

$$\mathbf{S}^*(x) \stackrel{\nu}{=} \Downarrow^*((\exists d \in \mathbf{SD}) \mathbf{II}(d, x) \wedge \mathbf{S}^*(2x - d))$$

The modification of the predicate for infinite Gray code is even simpler since only the decision $x \leq 0 \vee x \geq 0$ is subject to the operator \Downarrow^* :

$$\mathbf{G}^*(x) \stackrel{\nu}{=} (-1 \leq x \leq 1) \wedge (x \neq 0 \rightarrow \Downarrow^*(x \leq 0 \vee x \geq 0)) \wedge \mathbf{G}^*(\mathbf{t}(x))$$

This means that extracted realisers are ordinary streams, however with concurrently computed digits.

Another central objective of the present paper is to do a similar thing for the hyperspace of non-empty compact subsets of \mathbb{I} . That is, we give a co-inductive characterisation of this space from which a Gray code-like representation of the non-empty compact subsets of \mathbb{I} can be extracted and compare it with the characterisation of the hyperspace of non-empty compact subsets of digit spaces investigated in [BS16, Sp21], now applied to the digit space $(\mathbb{I}, \mathbf{SD})$.

The analogue of the signed digit representation for compact sets is

$$\mathbf{S}_{\mathbf{K}}(K) \stackrel{\nu}{=} \mathbf{K}(K) \wedge (\exists E \in \mathbf{P}_{\mathbf{fin}}(\mathbf{SD})) K \subseteq \mathbf{II}_E \wedge (\forall d \in E)(K_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d]))$$

where \mathbf{K} is an atomic predicate characterising (axiomatically) the non-empty compact subsets of \mathbb{I} , $\mathbf{P}_{\mathbf{fin}}(\mathbf{SD})$ is the set of non-empty subsets of the signed digit set \mathbf{SD} , \mathbf{II}_E is the set of all points that are 1/2 close to the half of some digit in E , and K_d is the set of points in K that are 1/2 close to $d/2$ (e.g. $K_1 = K \cap [0, 1]$); finally, \mathbf{av}_d^{-1} is the inverse of the digit function $\lambda x.(x + d)/2$ (see Definition 9.4).

The generalisation of infinite Gray code of compact sets is trickier. Here, we compute the Gray codes of the minimum and maximum of K and then, recursively, narrow down the set (Definition 10.1):

$$\mathbf{G}_{\mathbf{K}}(K) \stackrel{\nu}{=} \mathbf{K}(K) \wedge \mathbf{G}(\mathbf{min} K) \wedge \mathbf{G}(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC})(K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])).$$

It is not hard to see that both definitions are generalisations of the point case, that is, $\mathbf{S}(x)$ exactly if $\mathbf{S}_{\mathbf{K}}(\{x\})$, and $\mathbf{G}(x)$ exactly if $\mathbf{G}_{\mathbf{K}}(\{x\})$. We give a constructive proof that

$\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}}$ from which a translation between the respective representations of compact sets can be extracted, thus lifting the corresponding result in [BT21a] from points to the compact sets.

Finally, we also lift the equation $\mathbf{S}^* = \mathbf{G}^*$ from points to compact sets. The definitions of the concurrent versions of $\mathbf{S}_{\mathbf{K}}(K)$ and $\mathbf{G}_{\mathbf{K}}(K)$ are obtained by putting stars at appropriate places (see Definition 9.9 and the beginning of Section 11):

$$\begin{aligned} \mathbf{S}_{\mathbf{K}}^*(K) &\stackrel{\nu}{=} \mathbf{K}(K) \wedge \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) K \subseteq \mathbf{I}_E \wedge (\forall d \varepsilon E)(K_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[K_d]))) \\ \mathbf{G}_{\mathbf{K}}^*(K) &\stackrel{\nu}{=} \mathbf{K}(K) \wedge \mathbf{G}^*(\mathbf{min} K) \wedge \mathbf{G}^*(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC})(K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[K_d])) \end{aligned}$$

Our final result is the equation $\mathbf{S}_{\mathbf{K}}^* = \mathbf{G}_{\mathbf{K}}^*$ which provides an equivalence of the concurrent signed digit and Gray code representations of non-empty compact sets.

An important proof tool in this work is *Archimedean Induction (AI)*, a formulation of the Archimedean property for real numbers as an induction principle introduced in [BT21b]. In the present paper we introduce different version of this principle which are vital for all our main results. Let us briefly discuss the main ideas.

Common formulations of the Archimedean property are either not realisable (e.g. $(\forall x)(\exists n \in \mathbb{N}) |x| \leq n$), or don't have computational content (e.g. $(\forall x)((\forall n \in \mathbb{N}) |x| < 2^{-n} \rightarrow x = 0)$). In contrast, the classically equivalent principle of Archimedean Induction (cf. Section 6)

$$\frac{(\forall x \neq 0) (|x| \leq 1/2 \rightarrow P(2x)) \rightarrow P(x)}{(\forall x \neq 0) P(x)} \quad (\text{AI})$$

inherits computational content from the (arbitrary) predicate P and is realised by general recursion. It is crucial that the variable x is not relativised to a predicate such as \mathbf{S} that would yield a representation of x . A simple example of an application of (AI) is $(\forall x, y \in \mathbf{S})(x + y \neq 0 \rightarrow (\exists n \in \mathbb{N})(|x| > 2^{-n} \vee |y| > 2^{-n}))$, which one would normally prove using the Archimedean property (in the form without computational content), countable choice (AC^ω) and Markov's principle (MP). Using (AI) one needs neither (AC^ω) nor (MP). Roughly speaking, (AI) can be viewed as a combination of all those three principles that avoids speaking about infinite sequences.

In this paper, we will use variants of (AI) and of the following classically equivalent but constructively slightly weaker form of (AI) which has another predicate B as parameter:

$$\frac{(\forall x \in B \setminus \{0\}) P(x) \vee (|x| \leq 1/2 \wedge B(2x) \wedge (P(2x) \rightarrow P(x)))}{(\forall x \in B \setminus \{0\}) P(x)} \quad (\text{AIB})$$

An example is a variant where both premise and conclusion are made concurrent (cf. Definition 6.1):

$$\frac{(\forall x \in B \setminus \{0\}) \Downarrow^*(P(x) \vee (|x| \leq 1/2 \wedge B(2x) \wedge (P(2x) \rightarrow P(x))))}{(\forall x \in B \setminus \{0\}) \Downarrow^*(P(x))} \quad (\text{CAIB}^*)$$

We also introduce versions of (AI) or (AIB) for compact sets (cf. Definition 9.1), signed digit represented compact sets (cf. Definition 9.5), and the restriction operator \upharpoonright (cf. Definition 9.7).

The paper is organised as follows: In Section 2 the definition of a digit space is recalled and extended Gray code introduced. Section 3 contains a short introduction to inductive and co-inductive definitions and the proof methods they come equipped with. The application to digit spaces is discussed as well.

The next two sections give brief introductions to the logical systems used for program extraction. Section 4 deals with *Intuitionistic Fixed Point Logic (IFP)* and the kind of realisability used to generate programs. We follow [BT21a] except that in the case-construct of the programming language we permit clauses with overlapping patterns (see Section 4.2). In Section 5, the extension of IFP to *Concurrent Fixed Point Logic (CFP)* is discussed. The logic contains two new connectives from [BT21b] and corresponding proof rules. The rules are all realisable. We will derive further rules.

In Section 6 and 7, respectively, concurrent versions of Archimedean induction and the predicates \mathbf{S} and \mathbf{G} are introduced. These predicates are such that the realisers of their elements are signed digit and/or Gray code representations of the elements. The concurrent versions of both predicates are shown to coincide. From the proofs computable translations between the two representations can be extracted.

The remaining sections deal with non-empty compact subsets of the interval \mathbb{I} . In Section 8 some facts presented in [BS16] about the representation of the non-empty compact subsets of a digit space by digit trees are recalled. These are finitely branching infinite trees. Their nodes are labelled with digits. The words along the infinite paths are codes of the elements of the represented compact set. In the special case of the non-empty compact subsets of \mathbb{I} , the representation is one-to-one, if the elements of \mathbb{I} are represented by infinite Gray code. Archimedean induction for the non-empty compact subsets of \mathbb{I} is discussed in Section 9.

In Section 10 a predicate $\mathbf{G}_{\mathbf{K}}$ is co-inductively defined the realisers of which are Gray code representations of the non-empty compact subsets of \mathbb{I} . A similar predicate $\mathbf{S}_{\mathbf{K}}$ was defined in the previous section with respect to the signed digit representation. It is shown that $\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}}$. Just as in the point case, for the converse inclusion a concurrent version $\mathbf{S}_{\mathbf{K}}^*$ of the predicate $\mathbf{S}_{\mathbf{K}}$ has to be considered. In Section 11, finally, a concurrent version $\mathbf{G}_{\mathbf{K}}^*$ of the predicate $\mathbf{G}_{\mathbf{K}}$ is introduced and the equality $\mathbf{S}_{\mathbf{K}}^* = \mathbf{G}_{\mathbf{K}}^*$ is derived. Again computable translations between the digital trees based on signed digit representation and Gray code representation, respectively, can be extracted from the proof.

Realisers are an important ingredient of the approach delineated so far: Results are derived by applying the logical rules of Concurrent Fixed Point logic as well as new rules provided in the paper. But the algorithms used in applications are obtained by following the proof rules and combining their realisers accordingly. For each of the results derived in the real number case, that is in Section 7, we will present the realisers obtained in this way. In the compact sets case we leave this to the reader as the proofs follow a pattern very similar to the point case.

A further crucial aspect of this work is abstraction: The logical language and proof calculus do not refer to the operational semantics of programs. Instead, operational soundness is guaranteed through a general computational adequacy theorem that applies to any concurrent operational semantics satisfying certain fairness requirements² [BT21b]. This means that extracted programs can be executed in any efficient concurrent execution model.

2. DIGIT SPACES

We review the concept of a digit space [BS16, Sp21] as a general model of computation with infinite streams of digits.

²Committing to a fixed operational semantics would make concurrent logical rules and programming constructs redundant since they could be sequentialised by familiar scheduling/dove-tailing techniques.

Definition 2.1. Let (X, μ) be a non-empty compact metric space and E be a finite collection of contracting self-maps $e: X \rightarrow X$. Then (X, E) is a *digit space*, if

$$X = \bigcup \{ e[X] \mid e \in E \}. \quad (2.1)$$

Here, $e[X] = \{ e(x) \mid x \in X \}$. The maps e will be called *digits* in this context.

Note that, being a continuous map on a compact set, the metric μ is bounded.

We identify a finite sequence of digits $\vec{e} = [e_0, \dots, e_{n-1}] \in E^n$ with the composition $e_0 \circ \dots \circ e_{n-1}$ and a digit e with the singleton sequence $[e] \in E^1$. The set of all finite sequences of digits will be denoted by $E^{<\omega}$. Moreover, we let E^ω be the set of all infinite sequences of elements of E and set for $\alpha \in E^\omega$,

$$\alpha^{<n} \stackrel{\text{Def}}{=} [\alpha_0, \dots, \alpha_{n-1}].$$

Lemma 2.2 [BS16, Lemma 2.3]. *Let (X, E) be a digit space. Then $\bigcap_{n \in \mathbb{N}} \alpha^{<n}[X]$ contains exactly one point which we denote by $[[\alpha]]$, for every $\alpha \in E^\omega$.*

The mapping $[[\cdot]]: E^\omega \rightarrow X$ is called the *coding map*.

As is well known, E^ω is a compact bounded metric space with metric

$$\delta(\alpha, \beta) = \begin{cases} 0 & \text{if } \alpha = \beta, \\ 2^{-\min\{n \mid \alpha_n \neq \beta_n\}} & \text{otherwise.} \end{cases}$$

Proposition 2.3 [BS16, Proposition 2.7].

- (1) *The coding map $[[\cdot]]$ is onto and uniformly continuous.*
- (2) *The metric topology in X is equivalent to the quotient topology induced by the coding map.*

Set

$$\alpha \sim \beta \iff [[\alpha]] = [[\beta]],$$

for $\alpha, \beta \in E^\omega$. Then \sim is an equivalence relation. The equivalence class associated with $\alpha \in E^\omega$ will be denoted by $[\alpha]_\sim$. Furnish the quotient E^ω/\sim with the quotient topology and let $q_\sim: E^\omega \rightarrow E^\omega/\sim$ be the quotient map. Moreover let $[[\cdot]]: E^\omega/\sim \rightarrow X$ be the uniquely determined continuous map with $[[\cdot]] \circ q_\sim = [[\cdot]]$.

Proposition 2.4. *The map $[[\cdot]]$ is a homeomorphism between the quotient E^ω/\sim and the metric space X .*

Proof. By construction $[[\cdot]]$ is a bijection. It remains to show that its inverse $[[\cdot]]^{-1}$ is continuous as well. Let A be a closed set in E^ω/\sim . Since X is compact and q_\sim continuous, it follows that E^ω/\sim is compact as well. Therefore, A is also compact and so is its continuous image $[[\widehat{A}]]$. As X is Hausdorff, we obtain that $[[\widehat{A}]]$ is closed, i.e., $(([[\cdot]])^{-1})^{-1}[A]$ is closed. \square

In what follows we will be interested in two sets of digits on the interval $\mathbb{I} \stackrel{\text{Def}}{=} [-1, +1] \subseteq \mathbb{R}$ furnished with the usual Euclidean metric.

Let $\text{AV} \stackrel{\text{Def}}{=} \{ \text{av}_i \mid i \in \text{SD} \}$ with $\text{SD} \stackrel{\text{Def}}{=} \{-1, 0, +1\}$ and

$$\text{av}_i(x) = (x + i)/2.$$

Then (\mathbb{I}, AV) is a digit space. Note that for $[i_0, \dots, i_{r-1}] \in \text{SD}^r$,

$$\text{range}(\text{av}_{i_0} \circ \dots \circ \text{av}_{i_{r-1}}) = \left[\sum_{\nu < r} i_\nu \cdot 2^{-(\nu+1)} - 1, \sum_{\nu < r} i_\nu \cdot 2^{-(\nu+1)} + 1 \right].$$

Hence, for $w \in \text{SD}^\omega$ and $\alpha_w \in \text{AV}^\omega$ with $\alpha_w(\nu) \stackrel{\text{Def}}{=} \text{av}_{w_\nu}$,

$$\llbracket \alpha_w \rrbracket = \sum_{\nu \geq 0} w_\nu \cdot 2^{-(\nu+1)},$$

that is w is a *signed digit representation* of $\llbracket \alpha_w \rrbracket$. Therefore, we call (\mathbb{I}, AV) *signed digit space*. It satisfies a stronger covering condition than (2.1), which is needed in the development of most of the theory presented in [BS16, Sp21]: (\mathbb{I}, AV) is well-covering.

Definition 2.5. A digit space (X, E) is *well-covering* if

$$X = \bigcup \{ \text{int}(e[X]) \mid e \in E \},$$

where $\text{int}(e[X])$ denotes the interior of $e[X]$.

The other digit set we are going to consider leads to an important example of a digit space that is not well-covering.

Let $\text{GF} \stackrel{\text{Def}}{=} \{ g_i \mid i \in \text{GC} \}$ with $\text{GC} \stackrel{\text{Def}}{=} \{-1, 1\}$ and

$$g_i(x) \stackrel{\text{Def}}{=} -i \cdot (x - 1)/2.$$

Then g_{-1} and g_1 are contractions with $g_{-1}[\mathbb{I}] = [-1, 0]$ and $g_1[\mathbb{I}] = [0, +1]$. However, $0 \notin [-1, 0) \cup (0, +1]$. Therefore,

Lemma 2.6. (\mathbb{I}, GF) is a digit space that is not well-covering.

Note that GC^ω is an extension of finite Gray code to infinite words.

By Proposition 2.3(2) we know that the metric topology on \mathbb{I} is equivalent to the quotient topology induced by the coding map $\llbracket \cdot \rrbracket_G$ associated with (\mathbb{I}, GF) . Set

$$\alpha \sim_G \beta \iff \llbracket \alpha \rrbracket_G = \llbracket \beta \rrbracket_G,$$

for $\alpha, \beta \in \text{GF}^\omega$.

Lemma 2.7. For $\alpha, \beta \in \text{GF}^\omega$, $\alpha \sim_G \beta$ if, and only if, either $\alpha = \beta$, or the following Properties (1-3) hold for some $i \geq 0$:

- (1) For all $j < i$, $\alpha_j = \beta_j$.
- (2) $\alpha_i = g_{-1}$ and $\beta_i = g_1$, or conversely, $\alpha_i = g_1$ and $\beta_i = g_{-1}$.
- (3) $\alpha_{i+1} = \beta_{i+1} = g_1$ and $\alpha_j = \beta_j = g_{-1}$, for all $j > i + 1$.

Proof. Without restriction assume that $\alpha \neq \beta$ and let $i \geq 0$ be such that $\alpha^{<i} = \beta^{<i}$, $\alpha_i = g_{-1}$ and $\beta_i = g_1$. Moreover, let $\alpha_{i+1} = g_1 = \beta_{i+1}$ as well as $\alpha_j = g_{-1} = \beta_j$, for all $j > i + 1$. Then we have for $n > 0$ that

$$\begin{aligned} g_{-1}^n[\mathbb{I}] &= [-1, 2^{-(n-1)} - 1], & (g_1 \circ g_{-1}^n)[\mathbb{I}] &= [1 - 2^{-n}, 1], \\ (g_{-1} \circ g_1 \circ g_{-1}^n)[\mathbb{I}] &= [-2^{-(n+1)}, 0], & \text{and } (g_1 \circ g_1 \circ g_{-1}^n)[\mathbb{I}] &= [0, 2^{-(n+1)}]. \end{aligned}$$

Therefore,

$$\{ \llbracket \alpha \rrbracket_G \} = \bigcap_{j \geq 0} \alpha^{<j}[\mathbb{I}] = \bigcap_{n \geq i} \alpha^{<i}[-2^{-(n+1)}, 0] \supseteq \alpha^{<i}[\bigcap_{n \geq i} [-2^{-(n+1)}, 0]] = \{ \alpha^{<i}(0) \},$$

from which it follows that $\llbracket \alpha \rrbracket_G = \alpha^{<i}(0)$. In the same way we obtain that $\llbracket \beta \rrbracket_G = \beta^{<i}(0)$. Hence, $\llbracket \alpha \rrbracket_G = \llbracket \beta \rrbracket_G$.

For the verification of the converse implication assume that $\alpha \neq \beta$. Then there is a smallest $i \geq 0$ so that $\alpha_i \neq \beta_i$. It follows that either $\alpha_i = g_{-1}$ and $\beta_i = g_1$, or conversely, $\alpha_i = g_1$ and $\beta_i = g_{-1}$. Without restriction we only consider the first case.

Assume that $\alpha_{i+1} = g_{-1}$. Then

$$[[\alpha]]_G \in \bigcap_{n>i} \alpha^{<n}[\mathbb{I}] \subseteq \alpha^{<i}[g_{-1}[g_{-1}[\mathbb{I}]]] = \alpha^{<i}[[-1, -1/2]].$$

If $\beta_{i+1} = g_{-1}$, we similarly obtain that

$$[[\beta]]_G \in \beta^{<i}[g_1[g_{-1}[\mathbb{I}]]] = \beta^{<i}[[1/2, 1]].$$

Since $[[\alpha]]_G = [[\beta]]_G$, $\alpha^{<i} = \beta^{<i}$, and the functions g_{-1} and g_1 are both one-to-one, it follows that

$$[[\alpha]]_G \in \alpha^{<i}[[-1, -1/2] \cap [1/2, 1]],$$

which is impossible.

On the other hand, if $\beta_{i+1} = g_1$, we have that $[[\beta]]_G \in \beta^{<i}[g_1[g_1[\mathbb{I}]]] = \beta^{<i}[[0, 1/2]]$, and hence that $[[\alpha]]_G \in \alpha^{<i}[[-1, -1/2] \cap [0, 1/2]]$, which is impossible as well.

It follows that $\alpha_{i+1} = g_1$, which means that $[[\alpha]]_G \in \alpha^{<i}[g_{-1}[g_1[\mathbb{I}]]] = \alpha^{<i}[[-1/2, 0]]$. Thus, $\beta_{i+1} = g_1$ as well.

Finally, suppose that there is a minimal $j > i + 1$ such that $\alpha_j = g_1$ and $\beta_{i+2} = \dots = \beta_{j-1} = g_{-1}$, or $\beta_j = g_1$ and $\alpha_{i+2} = \dots = \alpha_{j-1} = g_{-1}$. Again, we only consider the first case. Then

$$\alpha = \alpha_0 \dots \alpha_{i-1} g_{-1} g_1 g_{-1} \dots g_{-1} g_1 \alpha_{j+1} \dots \quad \text{and} \quad \beta = \beta_0 \dots \beta_{i-1} g_1 g_1 g_{-1} \dots g_{-1} \beta_j \beta_{j+1} \dots,$$

with $\alpha^{<i} = \beta^{<i}$. It follows that

$$\begin{aligned} [[\alpha]]_G \in \alpha^{<i}[g_{-1}[g_1[g_{-1}^{j-(i+2)}[g_1[\mathbb{I}]]]]] &= \alpha^{<i}[g_{-1}[g_1[g_{-1}^{j-(i+2)}[[0, 1]]]]] \\ &= \alpha^{<i}[g_{-1}[g_1[[-1 + 2^{i+2-j}, -1 + 2^{i+3-j}]]]] \\ &= \alpha^{<i}[g_{-1}[[1 - 2^{i+2-j}, 1 - 2^{i+1-j}]]] \\ &= \alpha^{<i}[[-2^{i+1-j}, -2^{i-j}]] \end{aligned}$$

and $[[\beta]]_G \in \alpha^{<i}[g_1[g_1[g_{-1}^{j-(i+2)}[\beta_j[\mathbb{I}]]]]]$.

Let us first consider the case that $\beta_j = g_1$. Then we have that

$$[[\beta]]_G \in \alpha^{<i}[g_1[[1 - 2^{i+2-j}, 1 - 2^{i+1-j}]]] = \alpha^{<i}[[2^{i-j}, 2^{i+1-j}]].$$

Hence, $[[\alpha]]_G \in \alpha^{<i}[[-2^{i+1-j}, -2^{i-j}] \cap [2^{i-j}, 2^{i+1-j}]]$, which is impossible.

If $\beta_j = g_{-1}$, we obtain that

$$\begin{aligned} [[\beta]]_G \in \alpha^{<i}[g_1[g_1[g_{-1}^{j-(i+2)}[g_1[\mathbb{I}]]]]] &= \alpha^{<i}[g_1[g_1[g_{-1}^{j-(i+2)}[[-1, 0]]]]] \\ &= \alpha^{<i}[g_1[g_1[[-1, 2^{i+2-j} - 1]]]] \\ &= \alpha^{<i}[g_1[[1 - 2^{i+1-j}, 1]]] \\ &= \alpha^{<i}[[0, 2^{i-j}]]. \end{aligned}$$

Thus, $[[\alpha]]_G \in \alpha^{<i}[[-2^{i+1-j}, -2^{i-j}] \cap [0, 2^{i-j}]]$, which is impossible again.

By symmetry we obtain similar contradictions in the other cases. \square

It follows that each equivalence class $[\alpha]_{\sim_G}$ contains at most two elements, and if so, then the two differ in exactly one place, which means that the information coming with this entry is not used in the computation of the coding map.

If $[\alpha]_{\sim_G} = \{\alpha\}$, then $\widehat{[[\alpha]_{\sim_G}]} = [[\alpha]]_G$. In the other case $[\alpha]_{\sim_G} = \{\alpha, \beta\}$ and there is some uniquely determined index $i \geq 0$ (also denoted by $i(\alpha)$) so that $\alpha = \alpha^{<i} g_{-1} g_1 g_{-1}^\omega$ and $\beta = \alpha^{<i} g_1 g_1 g_{-1}^\omega$, or vice versa. Then $\widehat{[[\alpha]_{\sim_G}]}_G = [[\alpha]]_G = [[\beta]]_G$ and hence

$$\begin{aligned} \widehat{[[\alpha]_{\sim_G}]}_G &= \{[[\alpha]]_G\} \cup \{[[\beta]]_G\} \\ &= \bigcap_{n \geq 0} \alpha^{<i} [g_{-1} [g_1 [g_{-1}^n [\mathbb{I}]]]] \cup \bigcap_{n \geq 0} \alpha^{<i} [g_1 [g_1 [g_{-1}^n [\mathbb{I}]]]] \\ &= \alpha^{<i} [g_{-1} [\bigcap_{n \geq 0} g_1 [g_{-1}^n [\mathbb{I}]]] \cup g_1 [\bigcap_{n \geq 0} g_1 [g_{-1}^n [\mathbb{I}]]]] \\ &= \alpha^{<i} [(g_{-1} \cup g_1) [\bigcap_{n \geq 0} g_1 [g_{-1}^n [\mathbb{I}]]]], \end{aligned}$$

where the multi-valued function $g_{-1} \cup g_1$ is defined by $(g_{-1} \cup g_1)(x) \stackrel{\text{Def}}{=} \{g_{-1}(x), g_1(x)\}$. Note that in this case for $Y \subseteq \mathbb{I}$,

$$(g_{-1} \cup g_1)[Y] = \bigcup \{(g_{-1} \cup g_1)(x) \mid x \in Y\} = \bigcup \{\{g_{-1}(x), g_1(x)\} \mid x \in Y\} = g_{-1}[Y] \cup g_1[Y].$$

Let $\perp \notin \text{GC}$ be a new symbol (\perp for *unspecified*) and $g_\perp \stackrel{\text{Def}}{=} g_{-1} \cup g_1$. It follows that

$$\widehat{[[\alpha]_{\sim_G}]}_G = \bigcap_{n \geq 0} \alpha^{<i} [g_\perp [g_1 [g_{-1}^n [\mathbb{I}]]]].$$

Set $\overline{\text{GF}} = \{g_\perp, g_{-1}, g_1\}$ and define $\Phi: \text{GF}^\omega \rightarrow \overline{\text{GF}}^\omega$ by

$$\Phi(\alpha) = \begin{cases} \alpha^{<i(\alpha)} g_\perp g_1 g_{-1}^\omega & \text{if } \|\alpha\| = 2, \\ \alpha & \text{otherwise.} \end{cases}$$

Then

$$\Phi(\alpha) = \Phi(\beta) \iff \alpha \sim_G \beta.$$

The elements of $\widehat{G} \stackrel{\text{Def}}{=} \text{range}(\Phi)$ are called *modified Gray code expansions* of the real numbers in \mathbb{I} , or just *Gray code* [Ts02]³. Topologise \widehat{G} with the topology co-induced by Φ . As we have seen earlier in this section, $\overline{\text{GF}}^\omega$ also possesses a canonical metric. Its restriction to \widehat{G} will be denoted by $\widehat{\delta}$, whereas δ denotes the corresponding metric on GF^ω . For $n \geq 0$, $\widehat{\alpha} \in \widehat{G}$ and $\alpha \in \text{GF}^\omega$, let $B_{\widehat{\delta}}(\widehat{\alpha}, 2^{-n})$ and $B_\delta(\alpha, 2^{-n})$ be the balls in \widehat{G} and GF^ω , respectively, of radius 2^{-n} around $\widehat{\alpha}$ and α .

Lemma 2.8. $\Phi^{-1}[B_{\widehat{\delta}}(\widehat{\alpha}, 2^{-n})] = \bigcup \{B_\delta(\beta, 2^{-n}) \mid \beta \in \Phi^{-1}[\{\widehat{\alpha}\}]\}$.

Proof. Three cases are to be considered.

Case $\widehat{\alpha}_m = g_\perp$, for some $m > n$. Then $\widehat{\alpha}_0, \dots, \widehat{\alpha}_n \in \text{GF}$ and hence, for any $\beta \in \Phi^{-1}[\{\widehat{\alpha}\}]$, $\beta_i = \widehat{\alpha}_i$, for $i \leq n$. Therefore, if $\gamma \in \Phi^{-1}[B_{\widehat{\delta}}(\widehat{\alpha}, 2^{-n})]$, i.e., if $\Phi(\gamma)^{<n+1} = \widehat{\alpha}^{<n+1}$, then $\gamma^{<n+1} = \beta^{<n+1}$, for any $\beta \in \Phi^{-1}[\{\widehat{\alpha}\}]$, which means that $\gamma \in B_\delta(\beta, 2^{-n})$, for any such β .

³Note that in recent research also words $\alpha \in \text{GF}^\omega$ with $\|\alpha\| = 2$ are considered as valid Gray code [BMST, BT21a].

Conversely, if $\gamma^{<n+1} = \beta^{<n+1}$, for some $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$, then $\Phi(\gamma)^{<n+1} = \Phi(\beta)^{<n+1} = \hat{\alpha}^{<n+1}$, i.e., $\Phi(\gamma) \in B_{\hat{\delta}}(\hat{\alpha}, 2^{-n})$.

Case $\hat{\alpha}_m = g_{\perp}$, for some $m \leq n$. It follows that $\hat{\alpha}_0, \dots, \hat{\alpha}_{m-1} \in \text{GF}$. Moreover, if $\gamma \in \Phi^{-1}[B_{\hat{\delta}}(\hat{\alpha}, 2^{-n})]$, then $\gamma^{<m} = \hat{\alpha}^{<m}$, $\gamma_{m+1} = g_1 = \hat{\alpha}_{m+1}$, $\gamma_j = g_{-1} = \hat{\alpha}_j$, for $m+1 < j \leq n$, and $\gamma_m = g_{-1}$ or $\gamma_m = g_1$. Set $\beta = \hat{\alpha}^{<m} \gamma_m g_1 g_{-1}^{\omega}$. Then $\gamma \in B_{\delta}(\beta, 2^{-n})$ and $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$.

Conversely, if $\gamma^{<n+1} = \beta^{<n+1}$, for some $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$, then $\Phi(\gamma)^{<n+1} = \Phi(\beta)^{<n+1} = \hat{\alpha}^{<n+1}$, which means that $\gamma \in \Phi^{-1}[B_{\hat{\delta}}(\hat{\alpha}, 2^{-n})]$.

Case $\hat{\alpha}_i \in \text{GF}$, for all $i \geq 0$. In this case we have for $\gamma \in \text{GF}^{\omega}$ that $\Phi(\gamma)^{<n+1} = \hat{\alpha}^{<n+1}$, exactly if $\gamma^{<n+1} = \hat{\alpha}^{<n+1}$, i.e., $\Phi^{-1}[B_{\hat{\delta}}(\hat{\alpha}, 2^{-n})] = B_{\delta}(\hat{\alpha}, 2^{-n})$. \square

This shows that the topology on \hat{G} co-induced by Φ is finer than the metric topology. We will now derive the converse.

Let $U \subseteq \hat{G}$ be open in the topology co-induced by Φ and $\hat{\alpha} \in U$. Then $\Phi^{-1}[U]$ is open in the metric topology on GF^{ω} and $\beta \in \Phi^{-1}[U]$, for all $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$. Note that the latter set is finite. Hence, there is some $n \geq 0$ so that for all $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$, $B_{\delta}(\beta, 2^{-n}) \subseteq \Phi^{-1}[U]$.

Lemma 2.9. $B_{\hat{\delta}}(\hat{\alpha}, 2^{-n}) \subseteq U$.

Proof. Similarly to the preceding proof we consider the following cases.

Case $\hat{\alpha}_i \in \text{GF}$, for all $i \geq 0$. Let $\beta \in \Phi^{-1}[\{\hat{\alpha}\}]$, then $\hat{\alpha} = \Phi(\beta) = \beta$ in this case, and hence $B_{\hat{\delta}}(\hat{\alpha}, 2^{-n}) \subseteq \Phi[B_{\delta}(\beta, 2^{-n})] \subseteq U$.

Case $\hat{\alpha}_m = g_{\perp}$, for some $m \geq 0$. Let $\beta, \tilde{\beta} \in \text{GF}^{\omega}$ such that $\beta_j = \tilde{\beta}_j = \hat{\alpha}_j$, for all $j \geq 0$ with $j \neq m$, $\beta_m = g_{-1}$, and $\tilde{\beta}_m = g_1$. Then $\{\beta, \tilde{\beta}\} = \Phi^{-1}[\{\hat{\alpha}\}]$. Hence, $B_{\delta}(\beta, 2^{-n}) \cup B_{\delta}(\tilde{\beta}, 2^{-n}) \subseteq \Phi^{-1}[U]$. Now, let $\hat{\gamma} \in B_{\hat{\delta}}(\hat{\alpha}, 2^{-n})$ and $\gamma \in \Phi^{-1}[\{\hat{\gamma}\}]$. Then $\gamma^{<n+1} = \beta^{<n+1}$ or $\gamma^{<n+1} = \tilde{\beta}^{<n+1}$, i.e., $\gamma \in B_{\delta}(\beta, 2^{-n}) \cup B_{\delta}(\tilde{\beta}, 2^{-n})$, from which we obtain that $\hat{\gamma} \in U$. Thus, $B_{\hat{\delta}}(\hat{\alpha}, 2^{-n}) \subseteq U$. \square

Proposition 2.10. *The metric topology on \hat{G} is equivalent to the topology co-induced by Φ .*

3. INDUCTIVE AND CO-INDUCTIVE DEFINITIONS

Let X be a set and $\mathcal{P}(X)$ its powerset. An operator $\Phi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ is *monotone* if for all $Y, Z \subseteq X$,

$$\text{if } Y \subseteq Z, \text{ then } \Phi(Y) \subseteq \Phi(Z);$$

and a set $Y \subseteq X$ is Φ -*closed* (or a pre-fixed point of Φ) if $\Phi(Y) \subseteq Y$. Since $\mathcal{P}(X)$ is a complete lattice, every monotone operator Φ has a least fixed point $\mu\Phi \in \mathcal{P}(X)$ by the Knaster-Tarski Theorem. We often write

$$P(x) \stackrel{\mu}{=} \Phi(P)(x),$$

instead of $P = \mu\Phi$. $\mu\Phi$ can be defined to be the least Φ -closed subset of X . Thus, we have the *induction principle* stating that for every $Y \subseteq X$,

$$\text{If } \Phi(Y) \subseteq Y \text{ then } \mu\Phi \subseteq Y.$$

Dual to inductive definitions are *co-inductive definitions*. A subset Y of X is called Φ -*co-closed* (or a post-fixed point of Φ) if $Y \subseteq \Phi(Y)$. By duality, every monotone Φ has a

largest fixed point $\nu\Phi$ which can be defined as the largest Φ -co-closed subset of Φ . So, we have the *co-induction principle* stating that for all $Y \subseteq X$,

$$\text{If } Y \subseteq \Phi(Y) \text{ then } Y \subseteq \nu\Phi.$$

Note that for $P \subseteq X$ we also write

$$P(x) \stackrel{\nu}{=} \Phi(P)(x)$$

instead of $P = \nu\Phi$.

For monotone operators $\Phi, \Psi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ define

$$\Phi \subseteq \Psi \stackrel{\text{Def}}{=} (\forall Y \subseteq X) \Phi(Y) \subseteq \Psi(Y).$$

It is easy to see that the operation ν is monotone, i.e., if $\Phi \subseteq \Psi$, then $\nu\Phi \subseteq \nu\Psi$. This allows to derive the following strengthening of the co-induction principle.

Lemma 3.1 (Strong Co-induction Principle [BT21a]). *Let $\Phi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ be a monotone operator. Then:*

$$\text{If } Y \subseteq \Phi(Y \cup \nu\Phi) \text{ then } Y \subseteq \nu\Phi.$$

The proof is dual to the proof of the strong induction principle in [BT21a, Sp21].

Lemma 3.2 (Generalised Half-strong Co-induction Principle). *Let $\Phi', \Phi: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ be monotone operators such that Φ' is absorbed by Φ , that is, $\Phi'(\Phi(Y)) \subseteq \Phi(Y)$ for all $Y \subseteq X$. Then:*

$$\text{If } Y \subseteq \Phi'(\Phi(Y) \cup \nu\Phi) \text{ then } Y \subseteq \nu\Phi.$$

Note: If Φ' is the identity, then this is the half-strong co-induction principle from [BT21a]. For a proof of that special case see [Sp21]. We will specialise generalised half-strong co-induction to a concurrent setting in Section 5 and use it in Section 7.

Proof. Assume $Y \subseteq \Phi'(\Phi(Y) \cup \nu\Phi)$. Since $\Phi(Y) \cup \nu\Phi \subseteq \Phi(Y \cup \nu\Phi)$ (by the monotonicity of Φ), we have $Y \subseteq \Phi'(\Phi(Y \cup \nu\Phi))$ (by the monotonicity of Φ'), and therefore $Y \subseteq \Phi(Y \cup \nu\Phi)$ since Φ' is absorbed by Φ . With strong co-induction, it follows $Y \subseteq \nu\Phi$. \square

The following example is taken from [Be17].

Example 3.3 (Natural numbers). Define $\Phi: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ by

$$\Phi(Y) := \{0\} \cup \{y + 1 \mid y \in Y\}.$$

Then $\mu\Phi = \mathbb{N} = \{0, 1, \dots\}$. The induction principle is logically equivalent to the usual zero-successor-induction on \mathbb{N} ; if $0 \in Y$ and $(\forall y \in Y)(y \in Y \rightarrow y + 1 \in Y)$, then $(\forall y \in \mathbb{N}) y \in Y$.

Example 3.4 (The set of non-empty finite subsets of a set). Let Y be a subset of a set X . Define $\Phi_Y: \mathcal{P}(\mathcal{P}(X)) \rightarrow \mathcal{P}(\mathcal{P}(X))$ by

$$\Phi_Y(Z) \stackrel{\text{Def}}{=} \{u \in \mathcal{P}(X) \mid (\exists x \in Y) u = \{x\} \vee (\exists v \in Z)(\exists y \in Y) u = v \cup \{y\}\}$$

and let $\mathbf{P}_{\text{fin}}(Y) \stackrel{\text{Def}}{=} \mu\Phi_Y$. Then $\mathbf{P}_{\text{fin}}(Y)$ is the set of all non-empty finite subsets of Y .

Example 3.5 (Digit Spaces). Digit spaces can be characterised co-inductively. Define $\mathbb{C}_X \subseteq X$ by

$$\mathbb{C}_X(x) \stackrel{\nu}{=} (\exists e \in E)(\exists y \in X) x = e(y) \wedge \mathbb{C}_X(y),$$

i.e. $\mathbb{C}_X = \nu\Phi_X$, where for $Z \subseteq X$,

$$\Phi_X(Z) \stackrel{\text{Def}}{=} \{x \in X \mid (\exists e \in E)(\exists y \in X) x = e(y) \wedge Z(y)\}.$$

Note here that we may consider subsets $A \subseteq X$ as unary predicates and write $A(x)$ instead of $x \in A$.

Lemma 3.6 [Sp21]. *Let (X, E) be a digit space. Then $X = \mathbb{C}_X$.*

If all digits $e \in E$ are invertible, a slightly more comfortable characterisation can be given. Define $\mathbb{C}'_X \subseteq X$ by

$$\mathbb{C}'_X(x) \stackrel{\nu}{=} (\exists e \in E) x \in \text{range}(e) \wedge \mathbb{C}'_X(e^{-1}(x)).$$

Lemma 3.7. *Let (X, E) be a digit space with only invertible digits. Then $\mathbb{C}'_X = \mathbb{C}_X$.*

Proof. Both inclusions follow by co-induction. Let $x \in \mathbb{C}'_X$. Then there exists $e \in E$ so that $x \in \text{range}(e)$ and $\mathbb{C}'_X(e^{-1}(x))$. It follows for $y = e^{-1}(x)$ that $x = e(y)$ and $\mathbb{C}'_X(y)$, which shows that $\mathbb{C}'_X \subseteq \Phi_X(\mathbb{C}'_X)$. Hence, $\mathbb{C}'_X \subseteq \mathbb{C}_X$.

Conversely, let $x \in \mathbb{C}_X$. Then there are $e \in E$ and $y \in X$ with $x = e(y)$ and $\mathbb{C}_X(y)$. It follows that $x \in \text{range}(e)$ and $\mathbb{C}_X(e^{-1}(x))$. Thus, $\mathbb{C}_X \subseteq \mathbb{C}'_X$. \square

Classically the set \mathbb{C}_X is rather uninteresting, but constructively it is significant, since from a constructive proof that $x \in \mathbb{C}_X$ one can extract a stream α of digits such that $x = \llbracket \alpha \rrbracket$.

For what follows let $S \stackrel{\text{Def}}{=} \mathbb{C}_{(\mathbb{I}, \text{AV})}$ and $G \stackrel{\text{Def}}{=} \mathbb{C}_{(\mathbb{I}, \text{GF})}$. Then

$$S(x) \stackrel{\nu}{=} (\exists i \in \text{SD}) \mathbb{I}(i, x) \wedge S(2x - i), \quad (3.1)$$

where for $i \in \text{SD}$ and $x \in \mathbb{I}$, $\mathbb{I}(i, x) \stackrel{\text{Def}}{=} |2x - i| \leq 1$, and

$$G(x) \stackrel{\nu}{=} (\exists j \in \text{GC}) x \in \text{range}(g_j) \wedge G(1 - j \cdot 2x). \quad (3.2)$$

Note that $\text{range}(g_{-1}) = [-1, 0]$ and $\text{range}(g_1) = [0, 1]$. Moreover, the functions $1 - 2(-x)$ and $1 - 2x$, respectively, form the left and the right branch of the *tent function* $t(x) \stackrel{\text{Def}}{=} 1 - 2|x|$. Hence the right-hand side in (3.2) is equivalent to

$$((x < 0 \wedge j = -1) \vee (x > 0 \wedge j = 1) \vee x = 0) \wedge G(t(x)).$$

However, the last disjunction is not decidable as the test for 0 is not computable. Since we want to work in a logic that allows extracting computable content from disjunctions, a (classically) equivalent formula of what we have just obtained is preferable

$$G(x) \stackrel{\nu}{=} (x \neq 0 \rightarrow x \leq 0 \vee x \geq 0) \wedge G(t(x)). \quad (3.3)$$

Example 3.8 (Well-founded induction). The principle of *well-founded induction* is an induction principle for elements in the accessible or well-founded part of a binary relation \prec . As shown in [BT21a], it is an instance of strictly positive induction. The *accessible part* of \prec is inductively defined by

$$\mathbf{Acc}_{\prec}(x) \stackrel{\mu}{=} (\forall y \prec x) \mathbf{Acc}_{\prec}(y),$$

that is, $\mathbf{Acc}_{\prec} = \mu\Phi$ where $\Phi(X) \stackrel{\text{Def}}{=} \{x \mid (\forall y \prec x) X(y)\}$. A predicate P is called *progressive* if $\Phi(P) \subseteq P$, that is, $\mathbf{Prog}_{\prec}(P)$ holds where

$$\mathbf{Prog}_{\prec}(P) \stackrel{\text{Def}}{=} (\forall x)((\forall y \prec x) P(y) \rightarrow P(x)).$$

Therefore, the principle of well-founded induction, which states that a progressive predicate holds on the accessible part of \prec , is a direct instance of the rule of strictly positive induction:

$$\frac{\mathbf{Prog}_{\prec}(P)}{\mathbf{Acc}_{\prec} \subseteq P} (\text{WFI}_{\prec}(P)).$$

In most applications P is of the form $A \rightarrow Q$. The progressivity of $P \rightarrow Q$ can equivalently be written as progressivity of P relativised to A ,

$$\mathbf{Prog}_{\prec,A}(P) \stackrel{\text{Def}}{=} (\forall x \in A)((\forall y \in A) (y \prec x \rightarrow P(y)) \rightarrow P(x)).$$

and the conclusion becomes $\mathbf{Acc}_{\prec} \cap A \subseteq P$

$$\frac{\mathbf{Prog}_{\prec,A}(P)}{\mathbf{Acc}_{\prec} \cap A \subseteq P} (\text{WFI}_{\prec,A}(P)).$$

Dually to the accessibility predicate one can define for a binary relation a path predicate

$$\mathbf{Path}_{\prec}(x) \stackrel{\text{Def}}{=} (\exists y \prec x) \mathbf{Path}_{\prec}(y),$$

that is, $\mathbf{Path}_{\prec} = \nu\Psi$ where $\Psi(X) \stackrel{\text{Def}}{=} \{x \mid (\exists y \prec x) X(y)\}$. Intuitively, $\mathbf{Path}_{\prec}(x)$ states that there is an infinite descending path $\dots x_2 \prec x_1 \prec x$.

With the axiom of choice and classical logic it can be shown that $\neg\mathbf{Path}_{\prec}(x)$ implies $\mathbf{Acc}_{\prec}(x)$.

4. EXTRACTING ALGORITHMIC CONTENT FROM CO-INDUCTIVE PROOFS

In this section we recast the theory of digit spaces in a constructive setting with the aim to extract programs that provide effective representations of certain objects or transformations between different representations. As the main results on this basis we will obtain effective transformations between the signed digit and the Gray code representations of \mathbb{I} and the hyperspace of non-empty compact subsets of \mathbb{I} , respectively, showing that the two representations are effectively equivalent. The method of program extraction is based on a version of realisability, and the main constructive definition and proof principles will be induction and co-induction. The advantage of the constructive approach lies in the fact that proofs can be carried out in a representation-free way. Constructive logic and the Soundness Theorem automatically guarantee that proofs are witnessed by effective and provably correct transformations on the level of representations.

4.1. The formal system IFP. As basis for program extraction from proofs we use *Intuitionistic Fixed Point Logic* (IFP) [BT21a], which is an extension of many-sorted first-order logic by inductive and co-inductive definitions, i.e., predicates defined as least and greatest fixed points of strictly positive operators. Here, an occurrence of an expression E is *strictly positive* (*s.p.*) in an expression F if that occurrence is not within the premise of an implication, and a predicate P is *strictly positive in a predicate variable* X if every occurrence of X in P is strictly positive. Strict positivity is a simple and sufficiently general

syntactic condition that ensures monotonicity and hence the existence of these fixed points, as discussed in Section 3.

Relative to the language specified the following kinds of expression are defined:

Formulas A, B : *Equations* $s = t$ (s, t terms of the same sort), $P(\vec{t})$ (P a predicate which is not an abstraction, \vec{t} a tuple of terms whose sorts fit the arity of P), *conjunction* $A \wedge B$, *disjunction* $A \vee B$, *implication* $A \rightarrow B$, *universal* and *existential quantification* $(\forall x) A$, $(\exists x) A$.

Predicates P, Q : *Predicate variables* X, Y, \dots (each of fixed arity), *predicate constants*, *abstraction* $\lambda \vec{x}. A$ (arity given by the variable tuple \vec{x}), $\mu \Phi, \nu \Phi$ (arities = arity of Φ).

Operators Φ : $\lambda X. P$ where P must be strictly positive in X and the arities of X and P must coincide. The arity of $\lambda X. P$ is this common arity.

Falsity is defined as **False** $\stackrel{\text{Def}}{=} \mu(\lambda X. X)()$ where X is a predicate variable of arity $()$.

Program extraction is performed via a ‘uniform’ realisability interpretation (Section 4.4). Uniformity concerns the interpretation of quantifiers: A formula $(\forall x) A(x)$ is realised uniformly by one object a that realises $A(x)$ for all x , so a may not depend on x . Dually, a formula $(\exists x) A(x)$ is realised uniformly by one object a that realises $A(x)$ for some x , so a does not contain a witness for x . Expressions (formulas, predicates, operators) that contain no disjunction and no free predicate variables are identical to their realisability interpretations and are called *non-computational* (*nc*). A slightly bigger class of expressions are *Harrop expressions*. These may contain disjunctions and free predicate variables but not at strictly positive positions. A Harrop formula may not be identical to its realisability interpretation, however they have at most one realiser which is trivial and which is represented by the program constant **Nil** (see Sections 4.2 and 4.4).

We highlight some feature that distinguish IFP from other approaches to program extraction.

Classical logic: Although IFP is based on intuitionistic logic a fair amount of classical logic is available. Soundness of realisability holds in the presence of any non-computational axioms that are classically true. This can be extended to Harrop axioms whose realisability interpretations (see 4.4) are classically true.

Sets: We add for every sort s a powersort $\mathcal{P}(s)$ and a (non-computational) element-hood relation constant ε of arity $(s, \mathcal{P}(s))$. In addition, for every Harrop formula $A(x)$ the comprehension axiom

$$(\exists u)(\forall x)(x \varepsilon u \leftrightarrow A(x))$$

is added. ($A(x)$ may contain free variables other than x .) The realisability interpretation of such a comprehension axiom is again a comprehension axiom and can hence be accepted as true. We will use the notation $\{x \mid A(x)\}$ for the element u of sort $\mathcal{P}(s)$ whose existence is postulated in the comprehension axiom above. Hence, we can define the empty set $\emptyset \stackrel{\text{Def}}{=} \{x \mid \mathbf{False}\}$, singletons $\{x\} \stackrel{\text{Def}}{=} \{y \mid y = x\}$, the classical union of two sets $u \cup v \stackrel{\text{Def}}{=} \{x \mid \neg(x \not\varepsilon u \wedge x \not\varepsilon v)\}$, the union of all members of a set of sets $\bigcup u \stackrel{\text{Def}}{=} \{x \mid (\exists y \varepsilon u) x \varepsilon y\}$, and the intersection of a class of sets defined by a predicate P of arity $(\mathcal{P}(s))$, $\bigcap P \stackrel{\text{Def}}{=} \{x \mid (\forall y \in P) x \varepsilon y\}$.

Note that the informal notion of ‘set’ used in Section 3 is represented in the formal system IFP in three different ways:

- (1) Sorts are names for abstract ‘ground’ sets. For example, s is a name for the abstract set of real numbers.

- (2) Terms of sort $\mathcal{P}(s)$ denote subsets of the ground set denoted by s . Elements of sort $\mathcal{P}(s)$ can be defined by comprehension, $\{x \mid A(x)\}$, which is restricted to nc formulas $A(x)$.
- (3) Predicates are expressions denoting subsets of the ground sets. Predicates can be constructed by λ -abstraction, $\lambda x. A(x)$ (also written $\{x \mid A(x)\}$), where $A(x)$ can be any formula.

By ‘set’ we will mean in the following always (2), that is ‘element of sort $\mathcal{P}(s)$ ’. The three concepts form an increasing hierarchy since the sort s corresponds to the set $\{x \mid \mathbf{True}\}$ and every set u corresponds to the predicate $\lambda x. x \varepsilon u$. Note that $x \varepsilon u$ is an nc formula while $x \in P$ (which is synonym for $P(x)$) has computational content if the predicate P has.

To clarify the distinction we formally recast the definition of ‘the set of finite subsets of a set’ (Example 3.4), which should now rather be called ‘the predicate of finite subsets of a predicate’: Let P be a predicate of arity (s) (s and P correspond to X and Y in 3.4). We define the predicate $\mathbf{P}_{\text{fin}}(P)$ of arity $(\mathcal{P}(s))$ as $\mu \Phi_P$ where the operator Φ_P of arity $(\mathcal{P}(s))$ is defined as $\Phi_P = \lambda Z. \lambda u. (\exists x \in P) u = \{x\} \vee (\exists v \in Z)(\exists y \in P) u = v \cup \{y\}$.

Abstract real numbers: In formalising the theory of real numbers, e.g., the set \mathbf{R} of real numbers is regarded as a sort ι . A predicate \mathbf{N} with $\mathbf{N}(x)$ if the real number x is a natural number, is introduced by induction as in Example 3.3. All arithmetic constants and functions we wish to talk about are admitted as constant or function symbols. The predicates $=$, $<$ and \leq are considered as non-computational. As axioms, any true disjunction-free formulas about real numbers can be chosen. As such, the axiom system \mathcal{A}_R consists of a disjunction-free formulation of the axioms of real-closed fields, equations for exponentiation, the defining axiom for \max , stability of $=$, \leq , $<$, as well as the Archimedean property \mathbf{AP} about the non-existence of real numbers greater than all natural numbers, and Brouwer’s Thesis for nc predicates

$$(\mathbf{BT}_{\text{nc}}) \quad (\forall x) (\neg \mathbf{Path}_{<}(x) \rightarrow \mathbf{Acc}_{<}(x)).$$

Compact sets: In order to be able to deal with the hyperspace of non-empty compact subsets of the compact real interval $[-1, 1]$, we also add a predicate constant \mathbf{K} of arity $(\mathcal{P}(\iota))$ to denote the elements of that hyperspace. We also add an axiom for the finite intersection property stating that the intersection of the members of a descending sequence in \mathbf{K} is not empty.

Partial computation: Like the majority of programming languages, IFP’s language of extracted programs admits general recursion and therefore partial, i.e., non-terminating computation.

Infinite computation: Infinite data, as they naturally occur in exact real number computation, can be represented by infinite computations. This is achieved by an operational semantics where computations may continue forever outputting arbitrarily close approximations to the complete (infinite) result at their finite stages.

The proof rules of IFP include the usual natural deduction rules for intuitionistic first-order logic with equality. In addition there are the following rules for strictly positive induction and co-induction: the closure and co-closure of the least and greatest fixed point, respectively, stated as assumption-free rules, and the induction as well as the co-induction principle.

4.2. Programs and their semantics. Extracted programs, i.e. realisers, are interpreted as elements of a Scott domain D defined by the recursive domain equation

$$D = (\mathbf{Nil} + \mathbf{Left}(D) + \mathbf{Right}(D) + \mathbf{Pair}(D \times D) + \mathbf{Fun}(D \rightarrow D))_{\perp},$$

where $D \rightarrow D$ is the domain of continuous functions from D to D , $+$ denotes the disjoint sum of partial orders, and $(\cdot)_{\perp}$ adds a new bottom element. \mathbf{Nil} , \mathbf{Left} , \mathbf{Right} , \mathbf{Pair} and \mathbf{Fun} denote the injections of the various components of the sum into D . \mathbf{Nil} , \mathbf{Left} , \mathbf{Right} , \mathbf{Pair} (but not \mathbf{Fun}) are called *constructors*.

D carries a natural partial order \sqsubseteq with respect to which it is a countably based *Scott domain* (*domain* for short), that is a bounded-complete algebraic directed-complete partial order with least element \perp and a basis of countably many compact elements [GHKLMS03]. An element of D is called *defined* if it is different from \perp . Hence, each defined element is of one of the forms \mathbf{Nil} , $\mathbf{Left}(-)$, $\mathbf{Right}(-)$, $\mathbf{Pair}(-, -)$, $\mathbf{Fun}(-)$.

Since domains are closed under suprema of increasing chains D contains not only finite but also infinite combinations of the constructors. For example, writing $a : b$ for $\mathbf{Pair}(a, b)$, an infinite sequence of domain elements $(d_i)_{i \in \mathbb{N}}$ is represented in D as the stream

$$d_0 : d_1 : \dots \stackrel{\text{Def}}{=} \sup_{n \in \mathbb{N}} \mathbf{Pair}(d_0, \mathbf{Pair}(d_1, \dots, \mathbf{Pair}(d_n, \perp) \dots)).$$

Because Scott domains and continuous functions form a Cartesian closed category, D can be equipped with the structure of a partial combinatory algebra (PCA, [GHKLMS03]) by defining a continuous application operation ab such that $ab \stackrel{\text{Def}}{=} f(b)$, if $a = \mathbf{Fun}(f)$, and $ab \stackrel{\text{Def}}{=} \perp$, otherwise, as well as combinators K and S satisfying $Kab = b$ and $Sabc = ac(bc)$ (where application associates to the left). In particular D has a continuous least fixed point operator which can be defined by Curry's Y -combinator or as the mapping $(D \rightarrow D) \ni f \mapsto \sup_n f^n(\perp) \in D$.

Besides the PCA structure the algebraicity of D will be used, that is, the fact that every element of D is the directed supremum of compact elements. Compact elements have a strongly finite character. The finiteness of compact element is captured by their defining property, saying that $d \in D$ is compact if for every directed set $A \subseteq D$, if $d \sqsubseteq \bigsqcup A$, then $d \sqsubseteq a$ for some $a \in A$, and the existence of a function assigning to every compact element a a *rank*, $\mathbf{rk}(a) \in \mathbb{N}$, satisfying

rk1: If a has the form $C(a_1, \dots, a_k)$ for a data constructor C , then a_1, \dots, a_k are compact and $\mathbf{rk}(a) > \mathbf{rk}(a_i)$, for $1 \leq i \leq k$.

rk2: If a has the form $\mathbf{Fun}(f)$, then for every $b \in D$, $f(b)$ is compact with $\mathbf{rk}(a) > \mathbf{rk}(f(b))$ and there exists a compact $b_0 \sqsubseteq b$ such that $\mathbf{rk}(a) > \mathbf{rk}(b_0)$ and $f(b_0) = f(b)$. Moreover, there are finitely many compact elements b_1, \dots, b_n with $\mathbf{rk}(b_i) < \mathbf{rk}(a)$ such that $f(b) = \bigsqcup \{f(b_i) \mid 1 \leq i \leq n \wedge b_i \sqsubseteq b\}$.

Elements of D are denoted by programs which are defined as in [BT21a] except that the case construct is more general since it allows overlapping patterns. For example, it is now possible to define the function parallel-or [Pl77]. Setting $\mathbf{True} = \mathbf{Left}(\mathbf{Nil})$, $\mathbf{False} = \mathbf{Right}(\mathbf{Nil})$ parallel-or can be defined as

$$\begin{aligned} \lambda c. \text{ case } c \text{ of } \{ & \mathbf{Pair}(\mathbf{True}, -) \rightarrow \mathbf{True}; \\ & \mathbf{Pair}(-, \mathbf{True}) \rightarrow \mathbf{True}; \\ & \mathbf{Pair}(\mathbf{False}, \mathbf{False}) \rightarrow \mathbf{False} \} \end{aligned}$$

which is not possible in the programming language defined in [BT21a]. We will need this greater expressivity in Section 5.

Formally, *Programs* are terms M, N, \dots of a new sort δ built up as follows:

$$\begin{aligned}
 \text{Programs } \ni M, N, L, R & ::= a, b \quad (\text{program variables}) \\
 & | \mathbf{Nil} \mid \mathbf{Left}(M) \mid \mathbf{Right}(M) \mid \mathbf{Pair}(M, N) \\
 & | \mathbf{case } M \mathbf{ of } \{Cl_1; \dots; Cl_n\} \\
 & | \lambda a. M \\
 & | MN \\
 & | \mathbf{rec } M \\
 & | \perp
 \end{aligned}$$

where in the case-construct the Cl_i are pairwise compatible clauses (see Definition 4.1 below). A *clause* is an expression of the form $P \rightarrow N$ where P is a pattern and N is a program. A *pattern* is either a constructor pattern or a function pattern. A *constructor pattern* is a program built from constructors and variables such that each variable occurs at most once. *Function patterns* are of the form $\mathbf{fun}(a)$ where a is a program variable.

Definition 4.1. Two clauses, $P_1 \rightarrow N_1$ and $P_2 \rightarrow N_2$, are *compatible* if for any substitutions θ_1, θ_2 , if $P_1\theta_1 =_\alpha P_2\theta_2$, then $N_1\theta_1 =_\alpha N_2\theta_2$ where $=_\alpha$ means α -equality, that is, equality up to renaming of bound variables.

Compatibility of clauses can be decided efficiently since it is enough to consider most general unifiers θ_1 and θ_2 .

The variables in P are considered as binders. Hence, the free variables of a clause $P \rightarrow N$ are the free variables of N that do not occur in P .

In [BT21a] only simple patterns containing one occurrence of one constructor are considered and two clauses are required to have different constructors. This is equivalent to allowing arbitrary pattern but requiring different clauses to have non-unifiable pattern.

Programs that are α -equal will be identified. Moreover, we will write $a \stackrel{\text{rec}}{=} M$ for $a \stackrel{\text{Def}}{=} \mathbf{rec}(\lambda a. M)$, and $ab \stackrel{\text{rec}}{=} M$ for $a \stackrel{\text{rec}}{=} \lambda b. M$.

Definition 4.2.

- (1) A program M *matches a constructor pattern* P if there is a substitution θ , called the *matching substitution*, such that $\text{dom}(\theta) = \text{FV}(P)$ and $P\theta = M$.
- (2) A program M *matches a function pattern* $\mathbf{fun}(a)$ if M is a λ -abstraction and in this case the matching substitution is $[a \mapsto M]$.
- (3) A program *matches a clause* $P \rightarrow N$ if it matches P .

Except for the case-construct, the denotational semantics of programs in D is defined as in [BT21a]. To define the denotation $\mathbf{case } M \mathbf{ of } \{\vec{Cl}\}$ we first define when a domain element d *matches* a pattern P and, if it does, the *matching environment* which has as domain the variables of the pattern.

- In the case of a constructor pattern P this is obvious and the matching environment η (if it exists) will satisfy $\llbracket P \rrbracket \eta = d$.
- The matches of a function pattern $\mathbf{fun}(a)$ are the domain elements of the form $\mathbf{Fun}(f)$ and the matching environment is $[a \mapsto \mathbf{Fun}(f)]$.

The denotation of a case program in an environment η , $\llbracket \mathbf{case } M \mathbf{ of } \{\vec{Cl}\} \rrbracket \eta$, is defined as follows:

Definition 4.3.

- (1) If $P \rightarrow N$ is a clause in $\vec{C}l$ such that $\llbracket M \rrbracket \eta$ matches P with matching environment η' , then $\llbracket \mathbf{case} M \mathbf{of} \{ \vec{C}l \} \rrbracket \eta = \llbracket N \rrbracket (\eta + \eta')$ where $\eta + \eta'$ is the environment obtained by overriding η with η' .
- (2) If no such matching is possible, then $\llbracket \mathbf{case} M \mathbf{of} \{ \vec{C}l \} \rrbracket \eta = \perp$.

Due to the compatibility condition the denotation is independent of the choice of the matching clause. This follows from the fact that two patterns P_1, P_2 are unifiable if and only if they have a common match and the most general unifiers are in a one-to-one correspondence with the matching environments of the common match.

Definition 4.4. A program is called a *value* if it is an abstraction or begins with a constructor.

Note that a closed program is a value exactly if it is a weak head normal form (whnf). Clearly, if M is a value, then $\llbracket M \rrbracket \eta \neq \perp$ for every environment η .

The following small-step operational semantics of closed programs is similar to the one in [BT21a]. The difference is due to the more general case expressions.

- i. $\mathbf{case} M \mathbf{of} \{ \dots; P \rightarrow N; \dots \} \rightsquigarrow N\theta$ if M matches P with matching substitution θ .
- ii. $(\lambda x. M) N \rightsquigarrow M[N/x]$.
- iii. $\mathbf{rec} M \rightsquigarrow M(\mathbf{rec} M)$.
- iv. $\frac{M \rightsquigarrow M'}{\mathbf{case} M \mathbf{of} \{ \vec{C}l \} \rightsquigarrow \mathbf{case} M' \mathbf{of} \{ \vec{C}l \}}$ if M doesn't match any clause in $\vec{C}l$.
- v. $\frac{M \rightsquigarrow M'}{MN \rightsquigarrow M'N}$ if M is not an abstraction.
- vi. $\frac{M_i \rightsquigarrow M'_i \ (i = 1, \dots, k)}{C(M_1, \dots, M_k) \rightsquigarrow C(M'_1, \dots, M'_k)}$.
- vii. $\lambda x. M \rightsquigarrow \lambda x. M$.

Lemma 4.5 [BT21a]. *Let M be a closed program.*

1. $M \rightsquigarrow M'$ for exactly one M' .
2. If $M \rightsquigarrow M'$, then $\llbracket M \rrbracket = \llbracket M' \rrbracket$.
3. $\llbracket M \rrbracket \neq \perp$ exactly if there is a hnf V such that $M \rightsquigarrow^* V$.

Proof. (1) holds by the compatibility condition for case-constructs. (2) is easy. The proof of (3) is as the proof of [BT21a, Lemma 33] for the case that M begins with a constructor, and an easy consequence of [BT21a, Lemma 32] for the case that M is a λ -abstraction. \square

4.3. Types. A type $\tau(E)$ is assigned to every IFP-formula and predicate E , where types are expressions defined by the grammar

$$\text{Types} \ni \rho, \sigma ::= \alpha \text{ (type variables)} \mid \mathbf{1} \mid \rho \times \sigma \mid \rho + \sigma \mid \rho \Rightarrow \sigma \mid \mathbf{fix} \alpha. \rho$$

where in $\mathbf{fix} \alpha. \rho$ the type ρ must be strictly positive in α . Types are interpreted by subdomains of D in an obvious way.

The idea is that for a formula A , $\tau(A)$ is the type of potential realisers. Expressions without computational content will receive type $\mathbf{1}$.

Intuitively, by saying that a program a is a *realiser* of a formula A , one means that a is a computational content of formula A . In intuitionistic logic, a proof of $A \vee B$ gives us

the evidence that A is true or B is true. The notion of realiser used in the present paper is designed by treating this as the primitive source of computational content. Therefore, we defined an expression *non-computational* (*nc*) if it contains neither disjunctions nor free predicate variables. A more general notion of an expression with trivial computational content is provided by the Harrop property. A formula is *Harrop* if it contains neither disjunctions nor free predicate variables at strictly positive positions. A predicate P is *X-Harrop*, if P is strictly positive in X and $P[\hat{X}/X]$ is Harrop for \hat{X} a predicate constant associated with X .

$$\begin{aligned}
\tau(P(\vec{t})) &= \tau(P) \\
\tau(A \wedge B) &= \tau(A) \times \tau(B) && (A, B \text{ non-Harrop}) \\
&= \tau(A) && (B \text{ Harrop}) \\
&= \tau(B) && (\text{otherwise}) \\
\tau(A \vee B) &= \tau(A) + \tau(B) \\
\tau(A \rightarrow B) &= \tau(A) \Rightarrow \tau(B) && (A, B \text{ non-Harrop}) \\
&= \tau(B) && (A \text{ Harrop}) \\
\tau(\diamond x A) &= \tau(A) && (\diamond \in \{\forall, \exists\}) \\
\tau(X) &= \alpha_X && (X \text{ a predicate variable}) \\
\tau(P) &= \mathbf{1} && (P \text{ a predicate constant}) \\
\tau(\lambda \vec{x}. A) &= \tau(A) \\
\tau(\square(\lambda X. P)) &= \mathbf{fix} \alpha_X. \tau(P) && (\square \in \{\mu, \nu\}, P \text{ not } X\text{-Harrop}) \\
&= \mathbf{1} && (\square \in \{\mu, \nu\}, P \text{ } X\text{-Harrop})
\end{aligned}$$

For example, $\tau(\mathbb{N}) = \mathbf{nat} \stackrel{\text{Def}}{=} \mathbf{fix} \alpha. \mathbf{1} + \alpha$, the type of unary natural numbers.

4.4. Realisability. Next, we define the notion that a program $a : \tau(A)$ is a *realiser* of a formula A . In order to formalise this notion and to provide a formal proof of its soundness, Berger and Tsuiki [BT21a] introduced an extension RIFP of IFP which in addition to the sorts of IFP contains the sort δ , denoting the domain D . For each IFP formula A they define an RIFP predicate $\mathbf{R}(A)$ of arity (δ) that specifies the set of domain elements that realise A . Similarly, for every non-Harrop predicate P of arity $(\vec{\sigma})$ a predicate $\mathbf{R}(P)$ of arity $(\vec{\sigma}, \delta)$, and every non-Harrop operator Φ of arity $(\vec{\sigma})$ an operator $\mathbf{R}(\Phi)$ of arity $(\vec{\sigma}, \delta)$ is defined. Note that instead of $\mathbf{R}(A)(a)$ we also write $a \mathbf{r} A$. Moreover, we write $\mathbf{r} A$ to mean $(\exists a) a \mathbf{r} A$.

Simultaneously, $\mathbf{H}(B)$ is defined, for Harrop formulas B , which expresses that B is realisable, however with trivial computational content \mathbf{Nil} . More precisely, we define a formula $\mathbf{H}(A)$ for every Harrop formula A , a predicate $\mathbf{H}(P)$ for every Harrop predicate P , and an operator $\mathbf{H}(\Phi)$ for every Harrop operator Φ . $\mathbf{H}(P)$ and $\mathbf{H}(\Phi)$, respectively, will be of the same arity as P and Φ .

$$\begin{aligned}
a \mathbf{r} A &= (a = \mathbf{Nil} \wedge \mathbf{H}(A)) && (A \text{ Harrop}) \\
a \mathbf{r} P(\vec{t}) &= \mathbf{R}(P)(\vec{t}, a) && (P \text{ non-H.}) \\
c \mathbf{r} (A \wedge B) &= (\exists a, b) (c = \mathbf{Pair}(a, b) \wedge a \mathbf{r} A \wedge b \mathbf{r} B) && (A, B \text{ non-H.}) \\
a \mathbf{r} (A \wedge B) &= a \mathbf{r} A \wedge \mathbf{H}(B) && (B \text{ Harrop}, A \text{ non-H.})
\end{aligned}$$

$$\begin{aligned}
b\mathbf{r}(A \wedge B) &= \mathbf{H}(A) \wedge b\mathbf{r} B && (A \text{ Harrop}, B \text{ non-H.}) \\
c\mathbf{r}(A \vee B) &= (\exists a)(c = \mathbf{Left}(a) \wedge a\mathbf{r} A) \vee (\exists b)(c = \mathbf{Right}(b) \wedge b\mathbf{r} B) \\
c\mathbf{r}(A \rightarrow B) &= c : \tau(A) \Rightarrow \tau(B) \wedge (\forall a)(a\mathbf{r} A \rightarrow (ca)\mathbf{r} B) && (A, B \text{ non-H.}) \\
b\mathbf{r}(A \rightarrow B) &= b : \tau(B) \wedge (\mathbf{H}(A) \rightarrow b\mathbf{r} B) && (A \text{ Harrop}, B \text{ non-H.}) \\
a\mathbf{r} \diamond x A &= \diamond x (a\mathbf{r} A) && (\diamond \in \{\forall, \exists\}, A \text{ non-H.}) \\
\mathbf{R}(X) &= \tilde{X} \\
\mathbf{R}(\lambda \vec{x}. A) &= \lambda(\vec{x}, a)(a\mathbf{r} A) && (A \text{ non-H.}) \\
\mathbf{R}(\square(\Phi)) &= \square(\mathbf{R}(\Phi)) && (\square \in \{\mu, \nu\}, \Phi \text{ non-H.}) \\
\mathbf{R}(\lambda X. P) &= \lambda \tilde{X}. \mathbf{R}(P) && (P \text{ non-H.}) \\
\mathbf{H}(P(\vec{t})) &= \mathbf{H}(P)(\vec{t}) && (P \text{ Harrop}) \\
\mathbf{H}(A \wedge B) &= \mathbf{H}(A) \wedge \mathbf{H}(B) && (A, B \text{ Harrop}) \\
\mathbf{H}(A \rightarrow B) &= \mathbf{r} A \rightarrow \mathbf{H}(B) && (B \text{ Harrop}) \\
\mathbf{H}(\diamond x A) &= \diamond x \mathbf{H}(A) && (\diamond \in \{\forall, \exists\}, A \text{ Harrop}) \\
\mathbf{H}(P) &= P && (P \text{ a predicate constant}) \\
\mathbf{H}(\lambda \vec{x}. A) &= \lambda \vec{x}. \mathbf{H}(A) && (A \text{ Harrop}) \\
\mathbf{H}(\square(\Phi)) &= \square(\mathbf{H}(\Phi)) && (\square \in \{\mu, \nu\}, \Phi \text{ Harrop}) \\
\mathbf{H}(\lambda X. P) &= \lambda X. \mathbf{H}_X(P) && (P \text{ } X\text{-Harrop})
\end{aligned}$$

For the last line recall that a predicate P is X -Harrop, if P is strictly positive in X and $P[\hat{X}/X]$ is Harrop for \hat{X} a predicate constant associated with X . In this situation $\mathbf{H}_X(P)$ stands for $\mathbf{H}(P[\hat{X}/X])[X/\hat{X}]$. The idea is that $\mathbf{H}_X(P)$ is the same as $\mathbf{H}(P)$ but considering X as a (non-computational) predicate constant.

Lemma 4.6 [BT21a].

1. If A is Harrop, then $\mathbf{H}(A) \leftrightarrow \mathbf{r} A$.
2. If E is an nc expression, then $\mathbf{H}(E) = E$, in particular $\mathbf{H}(\mathbf{False}) = \mathbf{False}$.

Example 4.7 (Realiser of induction and co-induction). Set

$$\begin{aligned}
f \circ g &\stackrel{\text{Def}}{=} \lambda a. f(g a), \\
[f + g] &\stackrel{\text{Def}}{=} \lambda c. \mathbf{case} \ c \ \mathbf{of} \ \{\mathbf{Left}(a) \rightarrow f a; \mathbf{Right}(b) \rightarrow g b\}.
\end{aligned}$$

Note that if $f : \rho \rightarrow \sigma$ and $g : \sigma \rightarrow \sigma'$, then $g \circ f : \rho \rightarrow \sigma'$, and if $f_1 : \rho_1 \rightarrow \sigma$ and $f_2 : \rho_2 \rightarrow \sigma$, then $[f_1 + f_2] : (\rho_1 + \rho_2) \rightarrow \sigma$.

Note also that for a s.p. non-Harrop operator Φ , and a non-Harrop predicate P .

$$\tau(\mu(\Phi)) = \tau(\nu(\Phi)) = \mathbf{fix} \ \tau(\Phi) \stackrel{\text{Def}}{=} \mathbf{fix} \ \alpha. \tau(\Phi)(\alpha)$$

For every s.p. type operator φ let $\mathbf{mon}_\varphi : (\alpha \rightarrow \beta) \rightarrow \varphi(\alpha) \rightarrow \varphi(\beta)$ be the canonical program such that for every s.p. operator Φ and all predicates P, Q (of fitting arity), $\mathbf{mon}_\tau(\Phi)$ realizes $(P \subseteq Q) \rightarrow \Phi(P) \subseteq \Phi(Q)$. Then \mathbf{mon}_φ is a polymorphic program whose type depends on the type variables α, β . These type variables may be substituted by any types ρ, σ . We sometimes write $\mathbf{mon}_\varphi^{\rho, \sigma}$ to indicate that we are interested in the typing obtained by this substitution, that is, $\mathbf{mon}_\varphi^{\rho, \sigma} : (\rho \rightarrow \sigma) \rightarrow \varphi(\rho) \rightarrow \varphi(\sigma)$. A similar convention applies to the polymorphic programs defined below, such as \mathbf{it}_φ , \mathbf{coit}_φ , etc., as well as to the

polymorphic constructors $\mathbf{Left}^{\alpha,\beta} : \alpha \rightarrow (\alpha + \beta)$, $\mathbf{Right}^{\alpha,\beta} : \beta \rightarrow (\alpha + \beta)$, and the identity function $\mathbf{id}^\alpha : \alpha \rightarrow \alpha$. Of course these programs do not depend on the superscripts but only on the subscript (if any).

To improve readability we will in the following omit the ‘ τ ’ from $\tau(A)$, $\tau(P)$ and $\tau(\Phi)$ and we write $\nu\Phi$ instead of $\nu(\Phi)$, etc. Hence for example, instead of writing

$$\mathbf{mon}_{\tau(\Phi)}^{\tau(P),\tau(\nu(\Phi))} : (\tau(P) \rightarrow \tau(\nu(\Phi))) \rightarrow \tau(\Phi)(\tau(P)) \rightarrow \tau(\Phi)(\tau(\nu(\Phi)))$$

we write

$$\mathbf{mon}_{\Phi}^{P,\nu\Phi} : (P \rightarrow \nu\Phi) \rightarrow \Phi(P) \rightarrow \Phi(\nu\Phi)$$

or even

$$\mathbf{mon}_{\Phi}^{P,\nu\Phi} : (P \rightarrow \nu\Phi) \rightarrow \Phi(P) \rightarrow \nu\Phi$$

since $\tau(\Phi)(\tau(\nu\Phi)) \equiv \tau(\nu\Phi)$.

Induction. If $s : \Phi(P) \rightarrow P$ realises $\Phi(P) \subseteq P$, then $\mathbf{it}_{\Phi}^P s$ realises $\mu\Phi \subseteq P$ where

$$\begin{aligned} \mathbf{it}_{\varphi} &: (\varphi(\alpha) \rightarrow \alpha) \rightarrow \mathbf{fix}(\varphi) \rightarrow \alpha, \\ \mathbf{it}_{\varphi} s &\stackrel{\text{Def}}{=} \mathbf{rec} \lambda f. s \circ \mathbf{mon}_{\varphi}^{\mathbf{fix}(\varphi),\alpha} f. \end{aligned}$$

Co-induction. If $s : P \rightarrow \Phi(P)$ realises $P \subseteq \Phi(P)$, then $\mathbf{coit}_{\Phi}^P s$ realises $P \subseteq \nu\Phi$ where

$$\begin{aligned} \mathbf{coit}_{\varphi} &: (\alpha \rightarrow \varphi(\alpha)) \rightarrow \alpha \rightarrow \mathbf{fix} \varphi, \\ \mathbf{coit}_{\varphi} s &\stackrel{\text{Def}}{=} \mathbf{rec} \lambda f. \mathbf{mon}_{\varphi}^{\alpha,\mathbf{fix} \varphi} f \circ s. \end{aligned}$$

Half-strong co-induction. If $s : P \rightarrow (\Phi(P) + \nu\Phi)$ realises $P \subseteq \Phi(P) \cup \nu\Phi$, then $\mathbf{hscoit}_{\Phi}^P s$ realises $P \subseteq \nu\Phi$ where

$$\begin{aligned} \mathbf{hscoit}_{\varphi} &: (\alpha \rightarrow (\varphi(\alpha) + \mathbf{fix} \varphi)) \rightarrow \alpha \rightarrow \mathbf{fix} \varphi \\ \mathbf{hscoit}_{\varphi} s &\stackrel{\text{Def}}{=} \mathbf{rec} \lambda f. [\mathbf{mon}_{\varphi}^{\alpha,\mathbf{fix} \varphi} f + \mathbf{id}^{\mathbf{fix} \varphi}] \circ s \end{aligned}$$

Strong co-induction. If $s : P \rightarrow (\Phi(P) + \nu\Phi)$ realises $P \subseteq \Phi(P \cup \nu(\Phi))$, then $\mathbf{scoit}_{\Phi}^P s$ realises $P \subseteq \nu\Phi$ where

$$\begin{aligned} \mathbf{scoit}_{\varphi} &: (\alpha \rightarrow \varphi(\alpha + \mathbf{fix} \varphi)) \rightarrow \alpha \rightarrow \mathbf{fix} \varphi, \\ \mathbf{scoit}_{\varphi} s &\stackrel{\text{Def}}{=} \mathbf{rec} \lambda f. \mathbf{mon}_{\varphi}^{\alpha+\mathbf{fix} \varphi,\mathbf{fix} \varphi} [f + \mathbf{id}^{\mathbf{fix} \varphi}] \circ s. \end{aligned}$$

Generalised half-strong co-induction. Assume Φ' is monotone.

Let $\mathbf{absorb}_{\Phi',\Phi}^\alpha : \Phi'(\Phi(\alpha)) \rightarrow \Phi(\alpha)$ realise $\Phi'(\Phi(Y)) \subseteq \Phi(Y)$ for all Y .

If $s : P \rightarrow \Phi'(\Phi(P) + \nu\Phi)$ realises $P \subseteq \Phi'(\Phi(P) \cup \nu(\Phi))$, then

$$\mathbf{hscoit}_\Phi (\mathbf{absorb}_{\Phi',\Phi} \circ \mathbf{mon}_{\Phi'} [\mathbf{mon}_\Phi \mathbf{Left} + \mathbf{mon}_\Phi \mathbf{Right}] \circ s)$$

realises $P \subseteq \nu\Phi$. This means that the realiser is a function $f : P \rightarrow \nu\Phi$ defined recursively by

$$\begin{aligned} f &\stackrel{\text{rec}}{=} \mathbf{mon}_\Phi^{P+\nu\Phi, \nu\Phi} [f + \mathbf{id}^{\nu\Phi}] \\ &\quad \circ \mathbf{absorb}_{\Phi',\Phi}^{P+\nu\Phi} \\ &\quad \circ \mathbf{mon}_{\Phi'}^{\Phi(P)+\nu\Phi, \Phi(P+\nu\Phi)} [\mathbf{mon}_\Phi^{P, P+\nu\Phi} \mathbf{Left}^{P, \nu\Phi} + \mathbf{mon}_\Phi^{\nu\Phi, P+\nu\Phi} \mathbf{Right}^{P, \nu\Phi}] \\ &\quad \circ s. \end{aligned}$$

Example 4.8 (Realiser of well-founded induction). The schema of well-founded induction, $\mathbf{WFI}_{\prec, A}(P)$, is realised as follows: If s realises $\mathbf{Prog}_{\prec, A}$ where P is non-Harrop, then $\mathbf{Acc}_{\prec} \cap A \subseteq P$ is realised by

- $\tilde{f} \stackrel{\text{rec}}{=} \lambda a. (s a (\lambda a'. \lambda b. \tilde{f} a'))$ if \prec and A are both non-Harrop,
- $\tilde{f} \stackrel{\text{rec}}{=} \lambda a. (s a \tilde{f})$ if \prec is Harrop and A is non-Harrop,
- $\tilde{c} \stackrel{\text{rec}}{=} s (\lambda b. \tilde{c})$ if \prec is non-Harrop and A is Harrop,
- $\mathbf{rec} s$ if \prec and A are both Harrop.

See [BT21a, Lemma 21] for a proof.

4.5. Soundness. The Soundness Theorem [BT21a] stating that provable formulas are realisable is the theoretical foundation for program extraction.

Theorem 4.9 (Soundness). *Let \mathcal{A} be a set of nc axioms. From an $\text{IFP}(\mathcal{A})$ proof of formula A one can extract a program $M : \tau(A)$ such that $M \mathbf{r} A$ is provable in $\text{RIFP}(\mathcal{A})$.*

More generally, let Γ be a set of Harrop formulas and Δ a set of non-Harrop formulas. Then, from an $\text{IFP}(\mathcal{A})$ proof of a formula A from the assumptions Γ, Δ one can extract a program M with $\text{FV}(M) \subseteq \vec{u}$ such that $\vec{u} : \tau(\Delta) \vdash M : \tau(A)$ and $M \mathbf{r} A$ are provable in $\text{RIFP}(\mathcal{A})$ from the assumptions $\mathbf{H}(\Gamma)$ and $\vec{u} \mathbf{r} \Delta$.

If one wants to apply this theorem to obtain a program realising formula A one must provide terms K_1, \dots, K_n realising the assumptions in Δ . Then it follows that the term $M(K_1, \dots, K_n)$ realises A , provably in RIFP. Because the program axioms of RIFP given in [BT21a] are correct with respect to the denotational semantics, a further consequence is that $M(K_1, \dots, K_n)$ is a correct realiser of A .

That realisers do actually *compute* witnesses is shown in [BT21a] by two *Computational Adequacy Theorems* that relate the denotational definition of realisability with a lazy operational semantics.

5. COMPUTATIONALLY MOTIVATED LOGICAL CONNECTIVES

Non-termination is a natural and fundamental phenomenon in computation. It is denotationally modelled in domain theory [GHKLMS03] and a logical account of it is Scott’s logic with an existence predicate [Sc79]. The Minlog system [Min11] supports the extraction of programs that may or may not terminate and keeps control of potential partiality through a logic with totality degrees. A limitation of programs extracted from proofs in Minlog, or other systems such as Coq [Let02], is that they are sequential. Having the possibility of running computations concurrently, on the other hand, can be very useful to get around partiality. If, e.g., M and N are two programs known to realise formula A under the assumption that condition B or $\neg B$ holds, respectively, then at least one of them is guaranteed to terminate. So running them concurrently and picking the result obtained first, will lead to a result realising A , provided that if M or N terminates then it realises A .

To capture realisability restricted to a condition as described above, we follow the approach in [BT21b] and extend in Section 5.1 IFP by a propositional connective

$$A \upharpoonright_B \quad (\text{“}A \text{ restricted to } B\text{”})$$

which, for nc-formulas B , has a similar meaning as the formula $B \rightarrow A$ but behaves slightly differently (and better) with respect to realisability: While a realiser of $B \rightarrow A$ is a program that realises A if B holds but otherwise provides no guarantees, a realiser of $A \upharpoonright_B$ is a program p that terminates and realises A if B holds, but even if B does not hold, p will realise A provided p terminates. In order to behave well, the formation of $A \upharpoonright_B$ is restricted to formulas A satisfying a syntactic condition called productivity (defined in Section 5.1) that guarantees that only terminating programs can realise A .

In Section 5.2 we introduce the concurrency modality $\Downarrow(A)$ from [BT21b] with the crucial rule

$$\frac{A \upharpoonright_B \quad A \upharpoonright_{\neg B}}{\Downarrow(A)} \quad (\Downarrow\text{-lem})$$

that makes precise the above intuition. We also prove the realisability of a couple of further rules that say how \Downarrow interacts with other logical connectives.

Finally, in Section 5.3, we introduce a new concurrency modality, $\Downarrow^*(A)$, which inherits most of the properties of $\Downarrow(A)$ but in addition has realisable rules corresponding to a monad. This new modality will be used in Section 7 to define concurrent versions of the signed digit representation and infinite Gray code which are constructively equivalent.

5.1. Restriction $A \upharpoonright_B$. Following [BT21b], we introduce restriction, $A \upharpoonright_B$, where A is required to be *productive*⁴, that is, every implication and restriction in A has to be part of a Harrop formula or a disjunction. In particular, Harrop formulas and disjunctions are always productive. The reason why A is required to be productive is that this ensures that A has only defined realisers, that is \perp does not realise A .

The definition of the Harrop property is extended by demanding that Harrop formulas must not contain a restriction at a strictly positive position. In particular, restrictions are not Harrop. Realisability for restrictions is defined as

$$\mathbf{ar} A \upharpoonright_B \stackrel{\text{Def}}{=} a : \tau(A) \wedge (\mathbf{r} B \rightarrow a \neq \perp) \wedge (a \neq \perp \rightarrow \mathbf{ar} A).$$

⁴Observe that in [BT21b] the notion “strict” is used instead of “productive”.

Note that if A is a Harrop formula, then $a \mathbf{r} A \upharpoonright_B$ is equivalent to the formula

$$(\mathbf{r} B \vee a \neq \perp) \rightarrow (a = \mathbf{Nil} \wedge \mathbf{H}(A)).$$

The type of restriction is $\tau(A \upharpoonright_B) \stackrel{\text{Def}}{=} \tau(A)$.

To gain some intuition suppose that a closed program M realises $A \upharpoonright_B$. Since closed programs denote a value different from \perp exactly if they reduce to whnf, one has: (i) If B is realisable, then M reduces to whnf. (ii) If M reduces to whnf, then M realises A (even if B is not realisable). In this sense, one has partial correctness of M with respect to the specification A . The distinction between $A \upharpoonright_B$ and $B \rightarrow A$ regarding realisability is carefully discussed in [BT21b].

Sometimes, we need to get rid of the productivity requirement. This can be achieved by considering formulas of kind $A \vee \mathbf{False}$ instead of just A . By definition, $A \vee \mathbf{False}$ is always productive. Moreover, $a \mathbf{r} A$, exactly if $\mathbf{Left}(a) \mathbf{r} A \vee \mathbf{False}$. Note here that \mathbf{False} has no realiser. This leads us to the following unrestricted version of the restriction connective

$$A \upharpoonright_B^u \stackrel{\text{Def}}{=} (A \vee \mathbf{False}) \upharpoonright_B.$$

Since the realisers of such formulas are more complicated than those in the productive case, we keep both versions of the restriction connective. It should be clear from the definition that all statements in this paper about the realisability of rules for the restriction connective \upharpoonright also hold for the unrestricted version \upharpoonright^u .

The following derivation rules concerning restriction are added to IFP:

$$\frac{B \rightarrow A_0 \vee A_1 \quad \neg B \rightarrow A_0 \wedge A_1}{(A_0 \vee A_1) \upharpoonright_B} \quad (\upharpoonright\text{-intro } (A_0, A_1, B \text{ Harrop}))$$

$\frac{A}{A \upharpoonright_B} \quad (\upharpoonright\text{-return})$	$\frac{A \upharpoonright_B \quad A \rightarrow (A' \upharpoonright_B)}{A' \upharpoonright_B} \quad (\upharpoonright\text{-bind})$
$\frac{A \upharpoonright_B \quad B' \rightarrow B}{A \upharpoonright_{B'}} \quad (\upharpoonright\text{-antimon})$	$\frac{A \upharpoonright_B \quad B}{A} \quad (\upharpoonright\text{-mp})$
$\frac{}{A \upharpoonright_{\mathbf{False}}} \quad (\upharpoonright\text{-efq})$	$\frac{A \upharpoonright_B}{A \upharpoonright_{\neg B}} \quad (\upharpoonright\text{-stab})$
$\frac{(A \upharpoonright_B) \upharpoonright_C^u}{A \upharpoonright_{B \wedge C}} \quad (\upharpoonright\text{-absorb})$	$\frac{A \upharpoonright_B \quad C \upharpoonright_B}{(A \wedge C) \upharpoonright_B} \quad (\upharpoonright\text{-}\wedge).$

Lemma 5.1 [BT21b]. *The rules for restriction are realisable, provably in extended RIFP. Hence, Soundness Theorem 4.9 remains valid for the extension of IFP by restriction, however, classical logic is needed to derive the correctness of realisers.*

Note that the last two rules have not been considered in [BT21b]. As is easily verified, Rule ($\upharpoonright\text{-absorb}$) is realised by $\lambda a. \mathbf{case} a \mathbf{of} \{\mathbf{Left}(a') \rightarrow a'\}$ and Rule ($\upharpoonright\text{-}\wedge$) by $(\mathbf{Pair} \downarrow) \downarrow$, where $f \downarrow a$ denotes *strict application*:

$$f \downarrow a \stackrel{\text{Def}}{=} \mathbf{case} a \mathbf{of} \{C(-) \rightarrow f a \mid C \in \{\mathbf{Nil}, \mathbf{Left}, \mathbf{Right}, \mathbf{Pair}, \mathbf{fun}\}\}.$$

Observe that $f \downarrow a = f a$ if $a \neq \perp$ and $f \downarrow \perp = \perp$.

Lemma 5.2 [BT21b]. *The following rule is derivable from the rules for restriction:*

$$\frac{A \upharpoonright_B \quad A \rightarrow A'}{A' \upharpoonright_B} \text{ (}\upharpoonright\text{-mon)}.$$

The rule is realised by $\lambda f. \lambda a. f \downarrow a$. To see this assume that $a \mathbf{r} A \upharpoonright_B$ and $f \mathbf{r} (A \rightarrow A')$. We have to show that $f \downarrow a \mathbf{r} A' \upharpoonright_B$. Suppose first that $\mathbf{r} B$. Then $a \neq \perp$ and hence by definition of $f \downarrow$, $f \downarrow a = f a$. We need that $f a \neq \perp$. Here, the productivity requirement for the restriction connective comes into play: A' needs to be productive and since $f a \mathbf{r} A'$, we have that $f a \neq \perp$, as was to be shown. Next, suppose that $f \downarrow a \neq \perp$. Then $a \neq \perp$ as well, by definition of $f \downarrow$. Therefore, $a \mathbf{r} A$. It follows that $f a \mathbf{r} A'$. Since $a \neq \perp$, we moreover have that $f \downarrow a = f a$. Thus, $f \downarrow a \mathbf{r} A'$.

5.2. McCarthy's \mathbf{Amb} and the concurrency modality $\Downarrow(A)$. To deal with concurrency, [BT21b] introduced a further constructor $\mathbf{Amb}(a, b)$ indicating that its arguments a, b need be evaluated concurrently in order to obtain one of the results even if the other one is not terminating. The domain D now has to satisfy the domain equation

$$D = (\mathbf{Nil} + \mathbf{Left}(D) + \mathbf{Right}(D) + \mathbf{Pair}(D \times D) + \mathbf{Fun}(D \rightarrow D) + \mathbf{Amb}(D \times D))_{\perp}.$$

The programming language is extended by a constructor \mathbf{Amb} which denotes the constructor \mathbf{Amb} in the domain D . Hence, denotationally, the constructor \mathbf{Amb} is an exact copy of \mathbf{Pair} , that is, it acts like a lazy pairing operator. Only the operational semantics interprets a program $\mathbf{Amb}(M, N)$ as a concurrent computation of M and N until one of them is reduced to whnf. This is formalised by the following (non-deterministic) relation $\overset{c}{\rightsquigarrow}$ ('c' for 'choice'):

- ci. $\frac{M \rightsquigarrow M'}{M \overset{c}{\rightsquigarrow} M'}$,
- cii. $\mathbf{Amb}(M_1, M_2) \overset{c}{\rightsquigarrow} M_i$ if M_i is a whnf ($i = 1, 2$),
- ciii. $\frac{M_i \overset{c}{\rightsquigarrow} M'_i \ (i = 1, \dots, k)}{C(M_1, \dots, M_k) \overset{c}{\rightsquigarrow} C(M'_1, \dots, M'_k)}$ if $C \neq \mathbf{Amb}$.

The deterministic relation \rightsquigarrow which $\overset{c}{\rightsquigarrow}$ extends is now to be understood with respect to all constructors, including \mathbf{Amb} . The intuition of $\overset{c}{\rightsquigarrow}$ is that a program is first deterministically evaluated using \rightsquigarrow . If a program of the form $\mathbf{Amb}(M_1, M_2)$ is obtained, deterministic computation continues in parallel with M_1 and M_2 . As soon as one of the two programs reach a whnf, the other may be discarded using Rule (cii). Rule (ciii) says that the computation can be carried out inside (nested) data constructors. Note that rule (cii) cannot be applied to proper subterms of a term $\mathbf{Amb}(M_1, M_2)$ since the only way of reducing $\mathbf{Amb}(M_1, M_2)$ with a rule other than (cii) is by Rule (ci) and Rule (vi) of \rightsquigarrow . This ensures that at any point only two concurrent threads are needed to carry out the computation. For the reductions to yield the desired result (see [BT21b], Theorems 1 and 2), fairness conditions must be imposed. For example, if in $\mathbf{Amb}(M_1, M_2)$ at least one of the M_i is hnf, then Rule (cii) will eventually be applied. In [BT21b] slightly more general (and more complicated) but essentially equivalent rules are given which facilitate the formalisation of the fairness condition and allow parallel threads to be evaluated at different 'speeds'.

To indicate at the logical level that a realiser of a formula A may be computed concurrently, a new modality $\Downarrow(A)$ was introduced in [BT21b] where, again, the formula A is

required to be productive. For a non-Harrop formula A realisability is defined as

$$\begin{aligned} \mathbf{c}\mathbf{r} \Downarrow(A) &\stackrel{\text{Def}}{=} c = \mathbf{Amb}(a, b) \wedge a, b : \tau(A) \wedge \\ &\quad (a \neq \perp \vee b \neq \perp) \wedge \\ &\quad (a \neq \perp \rightarrow a \mathbf{r} A) \wedge (b \neq \perp \rightarrow b \mathbf{r} A). \end{aligned}$$

Thus, a realiser of $\Downarrow(A)$ is a pair of candidate realisers a and b at least one of which denotes a defined value and all of a and b which are defined values are correct realisers. In particular, if a and b are both defined, then they are *both* correct realisers. Therefore, by running the two programs for the candidates a and b concurrently and taking the one which becomes defined (i.e. a whnf) first, it is guaranteed that we obtain a correct result. Hence, we can safely stop the other process.

The occurrence of A in $\Downarrow(A)$ is regarded strictly positive. The definition of the Harrop property is further extended by demanding that Harrop formulas must not contain the concurrency operator at a strictly positive position. In particular, $\Downarrow(A)$ is always non-Harrop (even if A is Harrop). The type of the concurrency modality is $\tau(\Downarrow(A)) = \mathbf{A}(\tau(A))$ where \mathbf{A} is a new type operator.

IFP is once more extended by adding the following derivation rules. The logical system thus obtained is called *Concurrent Fixed Point Logic (CFP)*.

$$\frac{\begin{array}{c} \frac{A \uparrow_C \quad A \uparrow_{\neg C}}{\Downarrow(A)} \text{ (}\Downarrow\text{-lem)} \\ \frac{\Downarrow(A) \quad A \rightarrow B}{\Downarrow(B)} \text{ (}\Downarrow\text{-mon)} \\ \frac{\Downarrow(A \uparrow_B)}{\Downarrow(A)} \text{ (}\Downarrow\text{-}\uparrow\text{-absorb)} \end{array}}{\begin{array}{c} \frac{B \rightarrow \Downarrow(A_0 \vee A_1) \quad \neg B \rightarrow A_0 \wedge A_1}{\Downarrow(A_0 \vee A_1) \uparrow_B} \text{ (}\Downarrow\text{-}\uparrow\text{-intro (}A_0, A_1, B \text{ Harrop))} \end{array}} \left| \begin{array}{c} \frac{A}{\Downarrow(A)} \text{ (}\Downarrow\text{-return)} \\ \frac{\Downarrow(A)}{A} \text{ (}\Downarrow\text{-H (}A \text{ Harrop))} \\ \frac{A \uparrow_B \quad C \uparrow_D}{\Downarrow(A \vee C) \uparrow_{B \vee D}} \text{ (}\Downarrow\text{-}\uparrow\text{-}\vee) \end{array} \right.$$

Note that the last three rules have not been considered in [BT21b].

Lemma 5.3. *The rules for the concurrency modality are realisable.*

Proof. The realisability of the first four rules has been shown in [BT21b]. It remains to consider the last three rules.

It is easy to see that $(\Downarrow\text{-}\uparrow\text{-absorb})$ is realised by the identity function: Assume $\mathbf{c}\mathbf{r} \Downarrow(A \uparrow_B)$. Then $c = \mathbf{Amb}(a, b)$. Furthermore, $a \neq \perp$ or $b \neq \perp$, and in the first case $a \mathbf{r} A \uparrow_B$ while in the second case $b \mathbf{r} A \uparrow_B$. We show that $\mathbf{c}\mathbf{r} \Downarrow(A)$. By the facts we know about c , it suffices to show that if $a \neq \perp$ then $a \mathbf{r} A$ (and similarly for b). But if $a \neq \perp$, then $a \mathbf{r} A \uparrow_B$ and hence $a \mathbf{r} A$.

Next, we show that Rule $(\Downarrow\text{-}\uparrow\text{-}\vee)$ is realised by

$$g \stackrel{\text{Def}}{=} \lambda a. \lambda b. \mathbf{Amb}_{\mathbf{LR}}(\mathbf{Left} \downarrow a, \mathbf{Right} \downarrow b).$$

where $\mathbf{Amb}_{\mathbf{LR}}(u, v) \stackrel{\text{Def}}{=} \mathbf{Amb}(u, v)$ if $u = \mathbf{Left}(-)$ or $v = \mathbf{Right}(-)$ and $\stackrel{\text{Def}}{=} \perp$ otherwise. $\mathbf{Amb}_{\mathbf{LR}}$ can be easily defined using the case construct.

Suppose that $a \mathbf{r} A \uparrow_B$ and $b \mathbf{r} C \uparrow_D$. We have to verify that

1. $\mathbf{r}(B \vee D) \rightarrow gab \neq \perp$.
2. $gab \neq \perp \rightarrow (gab) \mathbf{r} \Downarrow(A \vee C)$.

(1) Assume $B \vee D$ is realisable. Then B or D is realisable. Without restriction assume $\mathbf{r}B$. Then $a \neq \perp$ and hence $\mathbf{Left}\downarrow a = \mathbf{Left}(a)$ and $gab = \mathbf{Amb}(\mathbf{Left}(a), \mathbf{Right}\downarrow b) \neq \perp$.

(2) If $gab \neq \perp$, then $gab = \mathbf{Amb}(u, v)$ where $u = \mathbf{Left}\downarrow a$ and $v = \mathbf{Right}\downarrow b$, and $u \neq \perp$ or $v \neq \perp$. Furthermore, if $u \neq \perp$, then $u = \mathbf{Left}(a)$ where $a \neq \perp$. Hence $a \mathbf{r}A$ and therefore $u \mathbf{r}(A \vee C)$. With a similar argument one sees that if $v \neq \perp$, then $v \mathbf{r}(A \vee C)$.

Rule ($\Downarrow\text{-}\uparrow\text{-intro}$), finally, is realised by

$$h \stackrel{\text{Def}}{=} \lambda c. \mathbf{case} \ c \ \mathbf{of} \ \{ \mathbf{Amb}(C(-), -) \rightarrow c; \mathbf{Amb}(-, C(-)) \rightarrow c \mid C \in \{ \mathbf{Left}, \mathbf{Right} \} \}.$$

Observe the overlapping clauses. First we note that for $c : \mathbf{A}(\tau(A_0 \vee A_1))$:

(*) : If c is of the form $\mathbf{Amb}(a, b)$, where $a \neq \perp$ or $b \neq \perp$, then $hc = c$. This is the case, in particular, if c realises $\Downarrow(A_0 \vee A_1)$.

(**): If $hc \neq \perp$, then $hc = c$ and c is of the form $\mathbf{Amb}(a, b)$ where $a \neq \perp$ or $b \neq \perp$.

Now, assume c realises $B \rightarrow \Downarrow(A_0 \vee A_1)$, that is, $c : \mathbf{A}(\tau(A_0 \vee A_1))$ and $\mathbf{H}(B) \rightarrow c \mathbf{r}(\Downarrow(A_0 \vee A_1))$, and that $\mathbf{H}(\neg B \rightarrow A_0 \wedge A_1)$ holds, that is, $\neg \mathbf{H}(B) \rightarrow \mathbf{H}(A_0) \wedge \mathbf{H}(A_1)$. We show that hc realises $\Downarrow(A_0 \vee A_1)\uparrow_B$:

First, assume $\mathbf{H}(B)$. Then c realises $\Downarrow(A_0 \vee A_1)$. Hence, by (*), $hc = c \neq \perp$.

Next, suppose $hc \neq \perp$. Then, by (**), $hc = c$ and c is of the form $\mathbf{Amb}(a, b)$ where $a \neq \perp$ or $b \neq \perp$. Therefore, it suffices to show that c realises $\Downarrow(A_0 \vee A_1)$. We do a classical case analysis on $\mathbf{H}(B)$. If $\mathbf{H}(B)$ holds, then c realises $\Downarrow(A_0 \vee A_1)$. If $\mathbf{H}(B)$ does not hold, then $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$ hold. To prove that c realises $\Downarrow(A_0 \vee A_1)$ it suffices to show that whenever a or b are defined, then they realise $A_0 \vee A_1$. Since $c : \mathbf{A}(\tau(A_0 \vee A_1))$, we have $a, b \in \tau(A_0 \vee A_1)$. But, since $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$ hold, every defined element in $\tau(A_0 \vee A_1)$ realises $A_0 \vee A_1$. \square

We summarise the realisers obtained by displaying the rules above with their realisers. We restrict Rule ($\Downarrow\text{-mon}$) to the most interesting cases where A and B are both non-Harrop. In this case we need for the rule the program

$$\mathbf{mapamb} \stackrel{\text{Def}}{=} \lambda f. \lambda c. \mathbf{case} \ c \ \mathbf{of} \ \{ \mathbf{Amb}(a, b) \rightarrow \mathbf{Amb}(f\downarrow a, f\downarrow b) \}.$$

$$\frac{\frac{\frac{a \mathbf{r}A\uparrow_C \quad b \mathbf{r}A\uparrow_{\neg C}}{\mathbf{Amb}(a, b) \mathbf{r} \Downarrow(A)} \ (\Downarrow\text{-lem}) \quad \frac{c \mathbf{r} \Downarrow(A) \quad f \mathbf{r}(A \rightarrow B)}{(\mathbf{mapamb} \ f \ c) \mathbf{r} \Downarrow(B)} \ (\Downarrow\text{-mon, } A, B \text{ non-Harrop})}{\frac{a \mathbf{r}A\uparrow_B \quad b \mathbf{r}C\uparrow_D}{(gab) \mathbf{r} \Downarrow(A \vee C)\uparrow_{B \vee D}} \ (\Downarrow\text{-}\uparrow\text{-}\vee)} \quad \left| \begin{array}{l} \frac{a \mathbf{r}A}{\mathbf{Amb}(a, \perp) \mathbf{r} \Downarrow(A)} \ (\Downarrow\text{-return}) \\ \frac{\mathbf{H}(\Downarrow(A))}{\mathbf{H}(A)} \ (\Downarrow\text{-H } (A \text{ Harrop})) \\ \frac{c \mathbf{r} \Downarrow(A\uparrow_B)}{c \mathbf{r} \Downarrow(A)} \ (\Downarrow\text{-}\uparrow\text{-absorb}) \end{array} \right.}{\frac{\mathbf{H}(B) \rightarrow c \mathbf{r} \Downarrow(A_0 \vee A_1) \quad \neg \mathbf{H}(B) \rightarrow \mathbf{H}(A_0) \wedge \mathbf{H}(A_1)}{(hc) \mathbf{r} \Downarrow(A_0 \vee A_1)\uparrow_B} \ (\Downarrow\text{-}\uparrow\text{-intro } (A_0, A_1, B \text{ Harrop}))}$$

where g, h are as defined in the proof.

Lemma 5.4. *The following rules are derivable in CFP:*

$$\frac{\neg\neg(A \vee B) \quad C \upharpoonright_A \quad C \upharpoonright_B}{\Downarrow(C)} (\Downarrow\text{-}\vee\text{-elim}) \quad \left| \quad \frac{\neg\neg(A \vee B) \quad C \upharpoonright_A \quad D \upharpoonright_B}{\Downarrow(C \vee D)} (\Downarrow\text{-}\vee\text{-elim-or}) \right.$$

$$\frac{\Downarrow(A \vee B)}{\Downarrow(\Downarrow(A) \vee \Downarrow(B))} (\Downarrow\text{-}\vee\text{-dist}) \quad \left| \quad \frac{\Downarrow(A \wedge B)}{\Downarrow(A) \wedge \Downarrow(B)} (\Downarrow\text{-}\wedge\text{-dist}). \right.$$

Proof. Rules $(\Downarrow\text{-}\vee\text{-elim})$ and $(\Downarrow\text{-}\vee\text{-elim-or})$ have already been considered in [BT21b]. The Rules $(\Downarrow\text{-}\vee\text{-dist})$ and $(\Downarrow\text{-}\wedge\text{-dist})$ are easy consequences of the Rules $(\Downarrow\text{-return})$ and $(\Downarrow\text{-mon})$. \square

Let us again display the rules with their realisers.

$$\frac{\neg\mathbf{H}(\neg(A \vee B)) \quad a \mathbf{r} C \upharpoonright_A \quad b \mathbf{r} C \upharpoonright_B}{\mathbf{Amb}(a, b) \mathbf{r} \Downarrow(C)} (\Downarrow\text{-}\vee\text{-elim})$$

$$\frac{\neg\mathbf{H}(\neg(A \vee B)) \quad a \mathbf{r} C \upharpoonright_A \quad b \mathbf{r} D \upharpoonright_B}{\mathbf{Amb}(\mathbf{Left}\downarrow a, \mathbf{Right}\downarrow b) \mathbf{r} \Downarrow(C \vee D)} (\Downarrow\text{-}\vee\text{-elim-or})$$

$$\frac{c \mathbf{r} \Downarrow(A \vee B)}{(\mathbf{mapamb} \ g \ c) \mathbf{r} \Downarrow(\Downarrow(A) \vee \Downarrow(B))} (\Downarrow\text{-}\vee\text{-dist})$$

where $g \ d \stackrel{\text{Def}}{=} \mathbf{case} \ d \ \mathbf{of} \ \{\mathbf{Left}(a) \rightarrow \mathbf{Left}(\mathbf{Amb}(a, \perp)); \mathbf{Right}(b) \rightarrow \mathbf{Right}(\mathbf{Amb}(b, \perp))\}$

$$\frac{c \mathbf{r} \Downarrow(A \wedge B)}{\mathbf{Pair}(\mathbf{mapamb} \ g_1 \ c, \mathbf{mapamb} \ g_2 \ c) \mathbf{r} \Downarrow(\Downarrow(A) \wedge \Downarrow(B))} (\Downarrow\text{-}\wedge\text{-dist})$$

where $g_i \ d \stackrel{\text{Def}}{=} \mathbf{case} \ d \ \mathbf{of} \ \{\mathbf{Pair}(a_1, a_2) \rightarrow \mathbf{Amb}(a_i, \perp)\}$.

5.3. The monadic concurrency modality $\Downarrow^*(A)$. It is easy to see that the concurrency modality \Downarrow is not a monad. The monadic lifting law $(A \rightarrow \Downarrow(B)) \rightarrow (\Downarrow(A) \rightarrow \Downarrow(B))$ is in general not realisable. In order to turn it into a monad we use its finite iterative closure

$$\Downarrow^*(A) \stackrel{\mu}{=} \Downarrow(A \vee \Downarrow^*(A)).$$

Note that $\Downarrow^*(A)$ is defined for arbitrary formulas A (not only productive ones) since in its definition \Downarrow is applied to a disjunction. As follows from the definition, we have for $c : \delta$,

$$c \mathbf{r} \Downarrow^*(A) \stackrel{\mu}{=} c = \mathbf{Amb}(a, b) \wedge a, b : \tau(A \vee \Downarrow^*(A)) \wedge (a \neq \perp \vee b \neq \perp) \wedge$$

$$(a \neq \perp \rightarrow (a = \mathbf{Left}(a') \wedge a' \mathbf{r} A) \vee (a = \mathbf{Right}(a'') \wedge a'' \mathbf{r} \Downarrow^*(A))) \wedge$$

$$(b \neq \perp \rightarrow (b = \mathbf{Left}(b') \wedge b' \mathbf{r} A) \vee (b = \mathbf{Right}(b'') \wedge b'' \mathbf{r} \Downarrow^*(A))).$$

As we will see next, in case of the iterated concurrency modality the following analogue of Rule $(\Downarrow\text{-}\upharpoonright\text{-intro})$ modality is realisable. Again A_0, A_1, B are required to be Harrop:

$$\frac{B \rightarrow \Downarrow^*(A_0 \vee A_1) \quad \neg B \rightarrow A_0 \wedge A_1}{\Downarrow^*(A_0 \vee A_1) \upharpoonright_B} (\Downarrow\text{-}\upharpoonright\text{-intro}).$$

We need the following functions $\sqcup_{\mathbf{Nil}, \triangleright} : D \times D \rightarrow D$ and $f^*, h^+, g : D \rightarrow D$:

$$\begin{aligned}
a \sqcup_{\mathbf{Nil}} b &\stackrel{\text{Def}}{=} \mathbf{case Pair}(a, b) \mathbf{ of } \{ \mathbf{Pair}(\mathbf{Nil}, -) \rightarrow \mathbf{Nil}; \mathbf{Pair}(-, \mathbf{Nil}) \rightarrow \mathbf{Nil} \}, \\
d \triangleright a &\stackrel{\text{Def}}{=} \mathbf{case } d \mathbf{ of } \{ \mathbf{Nil} \rightarrow a \}, \\
f^* d &\stackrel{\text{rec}}{=} \mathbf{case } d \mathbf{ of } \{ \mathbf{Left}(\mathbf{Left}(\mathbf{Nil})) \rightarrow \mathbf{Nil}; \\
&\quad \mathbf{Left}(\mathbf{Right}(\mathbf{Nil})) \rightarrow \mathbf{Nil}; \\
&\quad \mathbf{Right}(\mathbf{Amb}(u, v)) \rightarrow f^* u \sqcup_{\mathbf{Nil}} f^* v \}, \\
h^+ c &\stackrel{\text{rec}}{=} \mathbf{case } c \mathbf{ of } \{ \mathbf{Amb}(a, b) \rightarrow \\
&\quad \mathbf{case } f^* a \sqcup_{\mathbf{Nil}} f^* b \mathbf{ of } \{ \mathbf{Nil} \rightarrow \\
&\quad \quad \mathbf{Amb}(f^* a \triangleright g a, f^* b \triangleright g b) \} \\
&\quad \}, \\
g d &\stackrel{\text{Def}}{=} \mathbf{case } d \mathbf{ of } \{ \mathbf{Left}(-) \rightarrow d; \mathbf{Right}(e) \rightarrow \mathbf{Right}(h^+ e) \}.
\end{aligned}$$

Lemma 5.5. *Assume $A = A_0 \vee A_1$ where A_0 and A_1 are Harrop formulas.*

1. $(\forall a, b) (\mathbf{Amb}(a, b) \mathbf{r} \Downarrow^*(A) \rightarrow f^* a = \mathbf{Nil} \vee f^* b = \mathbf{Nil})$.
2. $(\forall c) (c \mathbf{r} \Downarrow^*(A) \rightarrow (h^+ c) \mathbf{r} \Downarrow^*(A))$.
3. *If $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$, then $(h^+ c) \mathbf{r} \Downarrow^*(A_0 \vee A_1)$, for all c such that $h^+ c$ is of the form $\mathbf{Amb}(-, -)$.*

Proof. (1) We use s.p. induction. If $\mathbf{Amb}(a, b) \mathbf{r} \Downarrow^*(A)$, then $a \mathbf{r} (A \vee \Downarrow^*(A))$, or $b \mathbf{r} (A \vee \Downarrow^*(A))$. Without restriction assume the former. If $a = \mathbf{Left}(d)$ where $d \mathbf{r} A$, then $f^* a = \mathbf{Nil}$. If $a = \mathbf{Right}(\mathbf{Amb}(u, v))$ where $\mathbf{Amb}(u, v) \mathbf{r} \Downarrow^*(A)$, then, by the induction hypothesis, $f^* u = \mathbf{Nil}$ or $f^* v = \mathbf{Nil}$. Hence $f^* a = \mathbf{Nil}$.

(2) Again, we use s.p. induction. Assume $c \mathbf{r} \Downarrow^*(A)$. Then, by (1), $c = \mathbf{Amb}(a, b)$ with $f^* a \sqcup_{\mathbf{Nil}} f^* b = \mathbf{Nil}$ and $h^+ c = \mathbf{Amb}(a', b')$ with $a' = f^* a \triangleright g a$ and $b' = f^* b \triangleright g b$. Since $f^* a \sqcup_{\mathbf{Nil}} f^* b = \mathbf{Nil}$, $a' = g a \neq \perp$ or $b' = g b \neq \perp$, as required. It remains to show that every defined element of $\{a', b'\}$ realises $A \vee \Downarrow^*(A)$. Without restriction let a' be defined. Hence $a' = g a$ and either (i) $g a = a = \mathbf{Left}(p)$ and thus $a' = \mathbf{Left}(p)$ with $p \in \{\mathbf{Left}(\mathbf{Nil}), \mathbf{Right}(\mathbf{Nil})\}$; or (ii) $a = \mathbf{Right}(q)$ and $g a = \mathbf{Right}(h^+ q)$, which means that $a' = \mathbf{Right}(h^+ q)$. Since $c \mathbf{r} \Downarrow^*(A)$ it follows that $a \mathbf{r} (A \vee \Downarrow^*(A))$. In Case (i), $a = a'$ and we are done since a is defined and hence realises $A \vee \Downarrow^*(A)$. In Case (ii), $q \mathbf{r} \Downarrow^*(A)$. Therefore, by the induction hypothesis, $(h^+ q) \mathbf{r} \Downarrow^*(A)$ and hence $a' \mathbf{r} (A \vee \Downarrow^*(A))$.

(3) Assume $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$. We prove the required formula first for compact c only and will later show that this is enough. Hence we show first

$$(\forall \text{ compact } c) (h^+ c = \mathbf{Amb}(-, -) \rightarrow (h^+ c) \mathbf{r} \Downarrow^*(A)).$$

We prove this by induction on the rank of c . The proof is in large parts similar to the proof of (2). Let c be compact and assume $h^+ c = \mathbf{Amb}(a', b')$. Then $c = \mathbf{Amb}(a, b)$ with $f^* a \sqcup_{\mathbf{Nil}} f^* b = \mathbf{Nil}$, $a' = f^* a \triangleright g a$ and $b' = f^* b \triangleright g b$. Since $f^* a \sqcup_{\mathbf{Nil}} f^* b = \mathbf{Nil}$, it

follows as in the proof of Statement (2) that $a' = ga \neq \perp$, or $b' = gb \neq \perp$. In either case, one of a', b' is defined, as required. It remains to show that every defined element of $\{a', b'\}$ realises $A \vee \Downarrow^*(A)$. Without restriction let a' be defined. Hence $a' = ga$ and either (i) $ga = a = \mathbf{Left}(p)$, and thus $a' = \mathbf{Left}(p)$ with $p \in \{\mathbf{Left}(\mathbf{Nil}), \mathbf{Right}(\mathbf{Nil})\}$; or (ii) $a = \mathbf{Right}(q)$ and $ga = \mathbf{Right}(h^+q)$, which means that $a' = \mathbf{Right}(h^+q)$. Since $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$, $\mathbf{Left}(\mathbf{Nil})$ and $\mathbf{Right}(\mathbf{Nil})$ both realise A . Hence, in Case (i), $a' \mathbf{r} (A \vee \Downarrow^*(A))$. In Case (ii), since $f^*a' = \mathbf{Nil}$, q must be of the form $\mathbf{Amb}(-, -)$. Therefore, since q has smaller rank than c , by the induction hypothesis, $(h^+q) \mathbf{r} \Downarrow^*(A)$ and hence $a' \mathbf{r} (A \vee \Downarrow^*(A))$.

To remove the restriction to compact c , it suffices to show that for every c there is a compact $c_0 \sqsubseteq c$ such that $h^+c_0 = h^+c$. If $h^+c = \perp$, then we can choose $c_0 = \perp$. Otherwise, $c = \mathbf{Amb}(a, b)$. Since f^* is continuous and its range contains only compact elements (namely \perp and \mathbf{Nil}), there are compact $a_0 \sqsubseteq a$ and $b_0 \sqsubseteq b$ such that $f^*a_0 = f^*a$ and $f^*b_0 = f^*b$. Therefore, it suffices to show

$$\begin{aligned} (\forall \text{ compact } a_0, b_0) (\forall a, b) (a_0 \sqsubseteq a \wedge b_0 \sqsubseteq b \wedge f^*(a_0) = f^*a \wedge f^*b_0 = f^*b \\ \rightarrow h^+ \mathbf{Amb}(a_0, b_0) = h^+ \mathbf{Amb}(a, b). \end{aligned}$$

This can be easily shown by induction on the maximum of the ranks of a_0 and b_0 . \square

Now, we are able to derive the result on Rule ($\Downarrow^* \text{-} \uparrow \text{-intro}$) we are aiming for.

Lemma 5.6. *Rule ($\Downarrow^* \text{-} \uparrow \text{-intro}$) is realised by h^+ .*

Proof. Set $A \stackrel{\text{Def}}{=} A_0 \vee A_1$, and assume that c realises $B \rightarrow \Downarrow^*(A)$ and $\mathbf{H}(\neg B \rightarrow A)$ holds. The former means that $\mathbf{H}(B) \rightarrow c \mathbf{r} \Downarrow^*(A)$ and the latter that $\neg \mathbf{H}(B) \rightarrow \mathbf{H}(A_0) \wedge \mathbf{H}(A_1)$. We have to show that h^+c realises $\Downarrow^*(A) \uparrow_B$.

First, assume $\mathbf{H}(B)$. Then $c \mathbf{r} \Downarrow^*(A)$ and, by Lemma 5.5(1), h^+c realises $\Downarrow^*(A)$ and is therefore defined.

Next, suppose h^+c is defined. Hence $c = \mathbf{Amb}(a, b)$ and $h^+c = \mathbf{Amb}(a', b')$ with $a' = f^*a \triangleright ga$ and $b' = f^*b \triangleright gb$. We have to show $(h^+c) \mathbf{r} \Downarrow^*(A)$. Since $\Downarrow^*(A)$ has the same realisers as $\Downarrow^*(A \vee \Downarrow^*(A))$, it is sufficient to derive that $(h^+c) \mathbf{r} \Downarrow^*(A \vee \Downarrow^*(A))$. That is, it suffices to verify that every defined element of $\{a', b'\}$ realises $A \vee \Downarrow^*(A)$. Without restriction assume that a' is defined. We do a classical case analysis on $\mathbf{H}(B)$. If $\mathbf{H}(B)$, then $c \mathbf{r} \Downarrow^*(A)$. Therefore, by Lemma 5.5(2), $(h^+c) \mathbf{r} \Downarrow^*(A)$ and hence $a' \mathbf{r} A \vee \Downarrow^*(A)$. If $\neg \mathbf{H}(B)$, then $\mathbf{H}(A_0)$ and $\mathbf{H}(A_1)$. By Lemma 5.5(3) we thus have that, $(h^+c) \mathbf{r} \Downarrow^*(A)$ and with the same argument as above we obtain $a' \mathbf{r} A \vee \Downarrow^*(A)$. \square

Similarly, an analogue of the well known introduction rule for the connective \wedge is realisable:

$$\frac{\Downarrow^*(A) \quad \Downarrow^*(B)}{\Downarrow^*(A \wedge B)} (\Downarrow^* \text{-} \wedge \text{-intro}).$$

Define

$$\begin{aligned} f^*d &\stackrel{\text{rec}}{=} \text{case } d \text{ of } \{\mathbf{Left}(_) \rightarrow \mathbf{Nil}; \mathbf{Right}(\mathbf{Amb}(u, v)) \rightarrow f^*u \sqcup_{\mathbf{Nil}} f^*v\}, \\ gde &\stackrel{\text{Def}}{=} \text{case } d \text{ of } \{\mathbf{Left}(d') \rightarrow \text{case } e \text{ of } \{\mathbf{Left}(e') \rightarrow \mathbf{Left}(\mathbf{Pair}(d', e')); \\ &\quad \mathbf{Right}(e'') \rightarrow \mathbf{Right}(h_2 d e'')\}; \\ &\quad \mathbf{Right}(d'') \rightarrow \mathbf{Right}(h_1 d'' e)\}, \end{aligned}$$

$$\begin{aligned} h_1 u v &\stackrel{\text{rec}}{=} \text{case } u \text{ of } \{\mathbf{Amb}(a, b) \rightarrow \\ &\quad \text{case } f^*a \sqcup_{\mathbf{Nil}} f^*b \text{ of } \{\mathbf{Nil} \rightarrow \mathbf{Amb}(f^*a \triangleright g a v, f^*b \triangleright g b v)\}\}, \end{aligned}$$

$$\begin{aligned} h_2 u v &\stackrel{\text{rec}}{=} \text{case } v \text{ of } \{\mathbf{Amb}(\bar{a}, \bar{b}) \rightarrow \\ &\quad \text{case } f^*\bar{a} \sqcup_{\mathbf{Nil}} f^*\bar{b} \text{ of } \{\mathbf{Nil} \rightarrow \mathbf{Amb}(f^*\bar{a} \triangleright g u \bar{a}, f^* \triangleright g u \bar{b})\}\}. \end{aligned}$$

Lemma 5.7.

1. $d \mathbf{r} A \wedge c \mathbf{r} \Downarrow^*(B) \rightarrow (h_2 \mathbf{Left}(d) c) \mathbf{r} \Downarrow^*(A \wedge B)$.
2. $c_1 \mathbf{r} \Downarrow^*(A) \wedge c_2 \mathbf{r} \Downarrow^*(B) \rightarrow (h_1 c_1 c_2) \mathbf{r} \Downarrow^*(A \wedge B)$.

Proof. Both statements are shown by s.p. induction.

(1) Assume that $d \mathbf{r} A$ and $c \mathbf{r} \Downarrow^*(B)$. Then $c = \mathbf{Amb}(\bar{a}, \bar{b})$ with $f^*\bar{a} \sqcup_{\mathbf{Nil}} f^*\bar{b} = \mathbf{Nil}$. Hence, $h_2 \mathbf{Left}(d) c = \mathbf{Amb}(a', b')$ with $a' = f^*\bar{a} \triangleright g d \bar{a}$ and $b' = f^*\bar{b} \triangleright g d \bar{b}$. Since $f^*\bar{a} \sqcup_{\mathbf{Nil}} f^*\bar{b} = \mathbf{Nil}$, we have that $a' \neq \perp$ or $b' \neq \perp$ as required. It remains to show that all defined elements of $\{a', b'\}$ realise $(A \wedge B) \vee \Downarrow^*(A \wedge B)$. Without restriction suppose that a' is defined. Recall that $d \mathbf{r} A$. So, we have that (i) $\bar{a} = \mathbf{Left}(p)$ with $p \mathbf{r} B$ and $g \mathbf{Left}(d) \mathbf{Left}(p) = \mathbf{Left}(\mathbf{Pair}(d, p))$, or (ii) $\bar{a} = \mathbf{Right}(q)$ and $g \mathbf{Left}(d) \bar{a} = \mathbf{Right}(h_2 \mathbf{Left}(d) q)$. Thus, $a' = \mathbf{Right}(h_2 \mathbf{Left}(d) q)$. Because $p \mathbf{r} B$, it follows in Case (i) that $\bar{a} \mathbf{r} (B \vee \Downarrow^*(B))$. Therefore, $(g \mathbf{Left}(d) \bar{a}) \mathbf{r} ((A \wedge B) \vee \Downarrow^*(A \wedge B))$, i.e., $(h_2 \mathbf{Left}(d) c) \mathbf{r} \Downarrow^*(A \wedge B)$.

In Case (ii) we have $q \mathbf{r} \Downarrow^*(B)$. By the induction hypothesis we therefore obtain that $(h_2 \mathbf{Left}(d) q) \mathbf{r} \Downarrow^*(A \wedge B)$. Thus, $a' \mathbf{r} ((A \wedge B) \vee \Downarrow^*(A \wedge B))$ which implies that

$$(h_2 \mathbf{Left}(d) c) \mathbf{r} \Downarrow^*(A \wedge B).$$

(2) Now, suppose that $c_1 \mathbf{r} A$ and $c_2 \mathbf{r} B$. Then $c_1 = \mathbf{Amb}(u, v)$ with $f^*u \sqcup_{\mathbf{Nil}} f^*v = \mathbf{Nil}$ and $h_1 c_1 c_2 = \mathbf{Amb}(a', b')$ with $a' = f^*u \triangleright g u c_2$ and $b' = f^*v \triangleright g v c_2$. Since $f^*u \sqcup_{\mathbf{Nil}} f^*v = \mathbf{Nil}$, we have that $a' = g u c_2 \neq \perp$ or $b' = g v c_2 \neq \perp$, as required. Again, it remains to show that each defined element of $\{a', b'\}$ realises $(A \wedge B) \vee \Downarrow^*(A \wedge B)$. Without restriction assume that a' is defined. Then $a' = g u c_2$ and (i) $u = \mathbf{Left}(d)$ with

$$g u c_2 = \text{case } c_2 \text{ of } \{\mathbf{Left}(e) \rightarrow \mathbf{Left}(\mathbf{Pair}(d, e)); \mathbf{Right}(e') \rightarrow \mathbf{Right}(h_2 u e')\},$$

or (ii) $u = \mathbf{Right}(d')$ and $g u c_2 = \mathbf{Right}(h_1 d' c_2)$, i.e., $a' = \mathbf{Right}(h_1 d' c_2)$.

In Case (i) it follows that either $a' = \mathbf{Left}(\mathbf{Pair}(d, e))$ and thus $a' \mathbf{r} ((A \wedge B) \vee \Downarrow^*(A \wedge B))$, or $a' = \mathbf{Right}(h_2 d e')$, from which we obtain with the first statement that again $a' \mathbf{r} ((A \wedge B) \vee \Downarrow^*(A \wedge B))$.

In Case (ii) we have that $d' \mathbf{r} \Downarrow^*(A)$ and hence by the induction hypothesis that $(h_1 d' c_2) \mathbf{r} \Downarrow^*(A \wedge B)$. Thus, $a' \mathbf{r} ((A \wedge B) \vee \Downarrow^*(A \wedge B))$, that is $(h_1 c_1 c_2) \mathbf{r} \Downarrow^*(A \wedge B)$. \square

Corollary 5.8. *Rule $(\Downarrow^*-\wedge\text{-intro})$ is realised by h_1 .*

We extend CFP by the Rules $(\Downarrow^*-\uparrow\text{-intro})$ and $(\Downarrow^*-\wedge\text{-intro})$.

Lemma 5.9. *The following rules for the iterated concurrency modality are derivable:*

$$\begin{array}{c}
 \frac{\Downarrow^*(A)}{A} \quad (\Downarrow^*\text{-H (A Harrop)}) \\
 \hline
 \begin{array}{|l}
 \frac{\Downarrow^*(A)}{\Downarrow^*(A)} \quad (\Downarrow^*\text{-emb}) \\
 \frac{A}{\Downarrow^*(A)} \quad (\Downarrow^*\text{-return}) \\
 \frac{\Downarrow^*(A \uparrow B)}{\Downarrow^*(A) \uparrow B} \quad (\Downarrow^*\text{-}\uparrow\text{-dist}) \\
 \frac{\Downarrow^*(A) \quad A \rightarrow B}{\Downarrow^*(B)} \quad (\Downarrow^*\text{-mon}) \\
 \frac{\Downarrow^*(A \rightarrow B)}{\Downarrow^*(A) \rightarrow \Downarrow^*(B)} \quad (\Downarrow^*\text{-}\rightarrow\text{-dist})
 \end{array}
 \quad
 \begin{array}{|l}
 \frac{\Downarrow^*(\Downarrow^*(A))}{\Downarrow^*(A)} \quad (\Downarrow^*\text{-}\Downarrow^*\text{-absorb}) \\
 \frac{\Downarrow^*(A) \quad A \rightarrow \Downarrow^*(A')}{\Downarrow^*(A')} \quad (\Downarrow^*\text{-bind}) \\
 \frac{\Downarrow^*(A \vee B)}{\Downarrow^*(\Downarrow^*(A) \vee \Downarrow^*(B))} \quad (\Downarrow^*\text{-}\vee\text{-dist}) \\
 \frac{\Downarrow^*(A \wedge B)}{\Downarrow^*(A) \wedge \Downarrow^*(B)} \quad (\Downarrow^*\text{-}\wedge\text{-dist}) \\
 \frac{\Downarrow^*(\Downarrow^*(A))}{\Downarrow^*(A)} \quad (\Downarrow^*\text{-idem}).
 \end{array}
 \end{array}$$

$$\frac{A \uparrow_{B_1} \dots A \uparrow_{B_n}}{\Downarrow^*(A) \uparrow_{B_1 \vee \dots \vee B_n}} \quad (\Downarrow^*\text{-}\uparrow\text{-}\vee)$$

Proof. Rule $(\Downarrow^*\text{-H})$ follows by induction. From $A \vee A \rightarrow A$ we obtain with Rules $(\Downarrow^*\text{-mon})$ and $(\Downarrow^*\text{-H})$ that $\Downarrow^*(A \vee A) \rightarrow \Downarrow^*(A)$ and $\Downarrow^*(A) \rightarrow A$, hence $\Downarrow^*(A \vee A) \rightarrow A$.

The Rules $(\Downarrow^*\text{-emb})$ and $(\Downarrow^*\text{-}\Downarrow^*\text{-absorb})$ follow directly from the definition of \Downarrow^* and Rule $(\Downarrow^*\text{-mon})$.

Rule $(\Downarrow^*\text{-return})$ follows directly from the definition of \Downarrow^* and the Rule $(\Downarrow^*\text{-return})$.

For Rule $(\Downarrow^*\text{-bind})$ assume that $A \rightarrow \Downarrow^*(A')$. We prove by induction that also $\Downarrow^*(A) \rightarrow \Downarrow^*(A')$, that is, we have to show that $\Downarrow^*(A \vee \Downarrow^*(A')) \rightarrow \Downarrow^*(A')$, which means that we must demonstrate that $\Downarrow^*(A \vee \Downarrow^*(A')) \rightarrow \Downarrow^*(A' \vee \Downarrow^*(A'))$. Because of the monotonicity of \Downarrow^* it suffices to prove that $A \vee \Downarrow^*(A') \rightarrow A' \vee \Downarrow^*(A')$, which is an immediate consequence of our assumption.

In case of Rule $(\Downarrow^*\text{-}\uparrow\text{-dist})$ we apply the induction principle again. It suffices to show $\Downarrow^*(A \uparrow_B \vee \Downarrow^*(A) \uparrow_B) \rightarrow \Downarrow^*(A) \uparrow_B$. With $(\Downarrow^*\text{-return})$ we have $A \rightarrow \Downarrow^*(A)$ and hence, because

of (\uparrow -*mon*), $A \uparrow_B \rightarrow \Downarrow^*(A) \uparrow_B$. Therefore, $(A \uparrow_B \vee \Downarrow^*(A) \uparrow_B) \rightarrow \Downarrow^*(A) \uparrow_B$, from which it follows with Rule (\Downarrow -*mon*) that $\Downarrow(A \uparrow_B \vee \Downarrow^*(A) \uparrow_B) \rightarrow \Downarrow(\Downarrow^*(A) \uparrow_B)$. With Rules (\Downarrow - \uparrow -*absorb*) and (\Downarrow - \Downarrow -*absorb*) we get $\Downarrow(A \uparrow_B \vee \Downarrow^*(A) \uparrow_B) \rightarrow \Downarrow^*(A) \uparrow_B$.

The Rules (\Downarrow - \vee -*dist*), (\Downarrow -*mon*), (\Downarrow - \wedge -*dist*), (\Downarrow - \rightarrow -*dist*), and (\Downarrow -*idem*) follow from the monadic laws (\Downarrow -*return*) and (\Downarrow -*bind*) in the usual way.

Rule (\Downarrow - \uparrow - \vee) is obtained, roughly speaking, by iterating Rule (\Downarrow - \uparrow - \vee). The proof is by induction on n . For $n = 1$, the rule follows immediately with Rules (\Downarrow -*return*) and (\uparrow -*mon*). For the step assume $A \uparrow_{B_1}, A \uparrow_{B_2}, \dots, A \uparrow_{B_{n+1}}$. By the induction hypothesis, $\Downarrow^*(A) \uparrow_{B_2 \vee \dots \vee B_{n+1}}$. With Rule (\Downarrow - \uparrow - \vee) it therefore follows $\Downarrow(A \vee \Downarrow^*(A)) \uparrow_{B_1 \vee B_2 \vee \dots \vee B_{n+1}}$. Since $\Downarrow(A \vee \Downarrow^*(A))$ is equivalent to $\Downarrow^*(A)$, we obtain $\Downarrow^*(A) \uparrow_{B_1 \vee B_2 \vee \dots \vee B_{n+1}}$ by applying Rule (\uparrow -*mon*). \square

The subsequent list contains realisers for the rules in the above lemma extracted from their proofs.

$$\begin{array}{c}
\frac{c \mathbf{r} \Downarrow^*(A)}{(\mathbf{mapamb} \text{ Left } c) \mathbf{r} \Downarrow^*(A)} \quad (\Downarrow^*\text{-emb}) \\
\frac{c \mathbf{r} \Downarrow^*(\Downarrow^*(A))}{(\mathbf{mapamb} \text{ Right } c) \mathbf{r} \Downarrow^*(A)} \quad (\Downarrow\text{-}\Downarrow\text{-absorb}) \\
\frac{a \mathbf{r} A}{(f_{\text{ret}} a) \mathbf{r} \Downarrow^*(A)} \quad (\Downarrow\text{-return, } f_{\text{ret}} \text{ below}) \\
\frac{c \mathbf{r} \Downarrow^*(A) \quad g \mathbf{r} (A \rightarrow \Downarrow^*(A'))}{(f_{\text{bind}} g c) \mathbf{r} \Downarrow^*(A')} \quad (\Downarrow\text{-bind, } f_{\text{bind}} \text{ below}) \\
\frac{c \mathbf{r} \Downarrow^*(A \uparrow_B)}{(f_{\uparrow\text{-dist}} c) \mathbf{r} \Downarrow^*(A) \uparrow_B} \quad (\Downarrow\text{-}\uparrow\text{-dist, } f_{\uparrow\text{-dist}} \text{ below}) \\
\frac{c \mathbf{r} \Downarrow^*(A) \quad g \mathbf{r} (A \rightarrow B)}{(f_{\text{mon}} g c) \mathbf{r} \Downarrow^*(B)} \quad (\Downarrow\text{-mon, } f_{\text{mon}} \text{ below}) \\
\frac{c \mathbf{r} \Downarrow^*(A \vee B)}{(f_{\text{mon}} (\mathbf{mapLR} f_{\text{ret}}) c) \mathbf{r} \Downarrow^*(\Downarrow^*(A) \vee \Downarrow^*(B))} \quad (\Downarrow\text{-}\vee\text{-dist}) \\
\frac{c \mathbf{r} \Downarrow^*(A \wedge B)}{\mathbf{Pair}(f_{\text{mon}} (\pi_L c), f_{\text{mon}} (\pi_R c)) \mathbf{r} (\Downarrow^*(A) \wedge \Downarrow^*(B))} \quad (\Downarrow\text{-}\wedge\text{-dist}) \\
\frac{c \mathbf{r} \Downarrow^*(A \rightarrow B)}{(f_{\text{bind}} (\lambda a. f_{\text{bind}} (\lambda f. f a) c)) \mathbf{r} (\Downarrow^*(A) \rightarrow \Downarrow^*(B))} \quad (\Downarrow\text{-}\rightarrow\text{-dist})
\end{array}$$

$$\frac{c \mathbf{r} \Downarrow^* (\Downarrow^* (A))}{(f_{\text{bind}} (\lambda a. a) c) \mathbf{r} \Downarrow^* (A)} \quad (\Downarrow^* \text{-idem})$$

$$\frac{b_1 \mathbf{r} A \upharpoonright_{B_1} \dots b_n \mathbf{r} A \upharpoonright_{B_n}}{(f_n b_1 \dots b_n) \mathbf{r} \Downarrow^* (A) \upharpoonright_{B_1 \vee \dots \vee B_n}} \quad (\Downarrow^* \upharpoonright \text{-}\vee)$$

where

$$f_{\text{ret}} a \stackrel{\text{Def}}{=} \mathbf{Amb}(\mathbf{Left}(a), \perp)$$

$$f_{\text{bind}} g \stackrel{\text{rec}}{=} \mathbf{mapamb} (\lambda d. \text{case } d \text{ of } \{\mathbf{Left}(a) \rightarrow \mathbf{Right}(g a); \mathbf{Right}(c') \rightarrow f_{\text{bind}} g c'\}),$$

$$f_{\upharpoonright \text{-dist}} \stackrel{\text{rec}}{=} \mathbf{mapamb} (\lambda d. \text{case } d \text{ of } \{\mathbf{Left}(a) \rightarrow d; \mathbf{Right}(c') \rightarrow f_{\upharpoonright \text{-dist}} c'\}),$$

$$f_{\text{mon}} g \stackrel{\text{rec}}{=} \mathbf{mapamb} (\lambda d. \text{case } d \text{ of } \{\mathbf{Left}(a) \rightarrow \mathbf{Left}(g a); \mathbf{Right}(c') \rightarrow f_{\text{mon}} g c'\}),$$

$$\mathbf{mapLR} g \stackrel{\text{Def}}{=} \lambda c. \text{case } c \text{ of } \{\mathbf{Left}(a) \rightarrow \mathbf{Left}(g a); \mathbf{Right}(b) \rightarrow \mathbf{Right}(g b)\},$$

$$\pi_L \stackrel{\text{Def}}{=} \lambda p. \text{case } p \text{ of } \{\mathbf{Pair}(a, -) \rightarrow a\},$$

$$\pi_R \stackrel{\text{Def}}{=} \lambda p. \text{case } p \text{ of } \{\mathbf{Pair}(-, b) \rightarrow b\},$$

$$f_1 b_1 \stackrel{\text{Def}}{=} f_{\text{ret}} \downarrow b_1,$$

$$f_{n+1} b_1 \dots b_{n+1} \stackrel{\text{Def}}{=} \bar{g} b_1 (f_n b_2 \dots b_{n+1}),$$

$$\bar{g} a c \stackrel{\text{Def}}{=} \mathbf{Amb}_{\text{LR}}(\mathbf{Left} \downarrow a, \mathbf{Right} \downarrow c).$$

A further useful rule that we will use in the sequel is a concurrent version of half-strong co-induction.

Lemma 5.10 (Concurrent Half-strong Co-induction Principle). *Let $\Phi_0: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ be a monotone operator and $\Phi(Y) \stackrel{\text{Def}}{=} \Downarrow^* (\Phi_0(Y))$. Then:*

$$\text{If } Y \subseteq \Downarrow^* (\Phi(Y) \cup \nu\Phi) \text{ then } Y \subseteq \nu\Phi.$$

The principle is an immediate consequence of the generalised half-strong co-induction principle (Lemma 3.2): Because of Rule $(\Downarrow^* \text{-mon})$ Φ is monotone and with Rule $(\Downarrow^* \text{-idem})$ we have that Φ absorbs \Downarrow^* . Note that $\tau(\Phi)(\alpha)$ is of the form $\mathbf{A}^*(\rho(\alpha))$. So, if $s : P \rightarrow \mathbf{A}^*(\Phi(P) + \nu\Phi)$ realises $P \subseteq \Downarrow^* (\Phi(P) \cup \nu\Phi)$, then $P \subseteq \nu\Phi$ is realised by $\mathbf{chscoit}_\Phi s : P \rightarrow \nu\Phi$ with

$$\mathbf{chscoit}_\Phi s \stackrel{\text{Def}}{=} f,$$

where f is defined as in the case of the realisability of generalised half-strong co-induction (Example 4.7). Moreover,

$$\mathbf{absorb}_{\Downarrow^*, \Phi}^\alpha \stackrel{\text{Def}}{=} f_{\text{bind}} (\lambda a. a) : \mathbf{A}^*(\Phi(\alpha)) \rightarrow \Phi(\alpha),$$

$$\mathbf{mon}_{\Downarrow^*} \stackrel{\text{Def}}{=} f_{\text{mon}}.$$

6. CONCURRENT ARCHIMEDEAN INDUCTION

A powerful tool in the investigation in [BT21a, BT21b] of the relationship between the signed digit representation and infinite Gray code is Archimedean induction, which is the Archimedean principle formulated as an induction rule:

$$\frac{(\forall x \neq 0) (|x| \leq 1/2 \rightarrow P(2x)) \rightarrow P(x)}{(\forall x \neq 0) P(x)} \text{ (AI)}$$

In IFP Rule(AI) is deduced as a special case of well-founded induction (cf. [BT21a]). A useful variant is:

$$\frac{(\forall x \in B \setminus \{0\}) P(x) \vee (|x| \leq 1/2 \wedge B(2x) \wedge (P(2x) \rightarrow P(x)))}{(\forall x \in B \setminus \{0\}) P(x)} \text{ (AIB)}$$

In what follows a concurrent version of the Rule (AIB) is needed.

Definition 6.1. *Iterated concurrent Archimedean induction* is the rule

$$\frac{(\forall x \in B \setminus \{0\}) \Downarrow^*(P(x) \vee (|x| \leq 1/2 \wedge B(2x) \wedge (P(2x) \rightarrow P(x))))}{(\forall x \in B \setminus \{0\}) \Downarrow^*(P(x))} \text{ (CAIB*)}$$

where B and P are non-Harrop predicates.

Lemma 6.2. *Rule (CAIB*) is realisable. Let s realise the premise of (CAIB*). Then $\mathbf{caibs} \stackrel{\text{Def}}{=} \lambda b. a(s b)$ realises the conclusion of (CAIB*), where a is defined by simultaneous recursion together with s' as*

$$\begin{aligned} a w &\stackrel{\text{rec}}{=} \mathbf{mapamb} \ s' w \\ s' u &\stackrel{\text{rec}}{=} \mathbf{case} \ u \ \mathbf{of} \ \{ \mathbf{Left}(\mathbf{Left}(c)) \rightarrow \mathbf{Left}(c); \\ &\quad \mathbf{Left}(\mathbf{Right}(\mathbf{Pair}(b, d))) \rightarrow \mathbf{Right}(f_{\text{bind}}(f_{\text{ret}} \circ d)(a(s b))); \\ &\quad \mathbf{Right}(w') \rightarrow \mathbf{Right}(a w') \}. \end{aligned}$$

Proof. $\lambda b. a(s b)$ has the right type, $\tau(B) \rightarrow \mathbf{A}^*(\tau(P))$ where $\mathbf{A}^*(\alpha) \stackrel{\text{Def}}{=} \mathbf{fix} \ \beta. \mathbf{A}(\alpha + \beta)$. This holds, since we have that $s : \tau(B) \rightarrow \mathbf{A}^*(\rho)$, with $\rho \stackrel{\text{Def}}{=} \tau(P) + \tau(B) \times (\tau(P) \rightarrow \tau(P))$, from which one can infer by a simple type inference that $a : \mathbf{A}^*(\rho) \rightarrow \mathbf{A}^*(\tau(P))$, and $s' : (\rho + \mathbf{A}^*(\rho)) \rightarrow (\tau(P) + \mathbf{A}^*(\tau(P)))$.

Set $C(x) \stackrel{\text{Def}}{=} P(x) \vee (|x| \leq 1/2 \wedge B(2x) \wedge (P(2x) \rightarrow P(x)))$. To complete the proof, it clearly suffices to show that if $x \neq 0$ and w realises $\Downarrow^*(C(x))$, then $a w$ realises $\Downarrow^*(P(x))$.

Let

$$Q(x) \stackrel{\text{Def}}{=} (\forall w) (w \mathbf{r} \Downarrow^*(C(x)) \rightarrow (a w) \mathbf{r} \Downarrow^*(P(x))).$$

We use Rule (AI) to prove that $(\forall x \neq 0) Q(x)$.

Let $x \neq 0$. The Archimedean induction hypothesis is

$$\mathbf{(AIH)}: |x| \leq 1/2 \rightarrow Q(2x).$$

We show $Q(x)$ by a side induction on the definition of $w \mathbf{r} \Downarrow^*(C(x))$. Hence we assume $w \mathbf{r} \Downarrow^*(C(x))$, that is, $w \mathbf{r} \Downarrow^*(C(x) \vee \Downarrow^*(C(x)))$, and have to derive that $a w$ realises $\Downarrow^*(P(x))$.

Thus, $w = \mathbf{Amb}(u, v)$ and $aw = \mathbf{Amb}(s'\downarrow u, s'\downarrow v)$. Furthermore, $u \neq \perp$ or $v \neq \perp$, hence $s'\downarrow u = s'u$ or $s'\downarrow v = s'v$. Moreover, for $k \in \{u, v\}$, if $k \neq \perp$ then

$$k \mathbf{r}(C(x) \vee \Downarrow^*(C(x))).$$

Before showing that $\mathbf{Amb}(s'\downarrow u, s'\downarrow v)$ realises $\Downarrow^*(P(x))$, we prove:

$$\text{If } k \in \{u, v\} \text{ such that } k \neq \perp, \text{ then } (s'k) \mathbf{r}(P(x) \vee \Downarrow^*(P(x))). \quad (6.1)$$

Without restriction assume $k = u \neq \perp$. Hence $u \mathbf{r}(C(x) \vee \Downarrow^*(C(x)))$ and $s'\downarrow u = s'u$.

If $u = \mathbf{Left}(\mathbf{Left}(c))$ with $c \mathbf{r} P(x)$, then $s'u = \mathbf{Left}(c)$, which means that $(s'u) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$.

If $u = \mathbf{Left}(\mathbf{Right}(\mathbf{Pair}(b, d)))$ with $|x| \leq 1/2$, $b \mathbf{r} B(2x)$ and $d \mathbf{r}(P(2x) \rightarrow P(x))$, then $s'u = \mathbf{Right}(f_{\text{bind}}(f_{\text{ret}} \circ d)(a(sb)))$. Moreover, by (AIH), $a(sb)$ realises $P(2x)$. Therefore, since $f_{\text{ret}} \circ d$ realises $(P(2x) \rightarrow \Downarrow^*(P(x)))$, we have that $f_{\text{bind}}(f_{\text{ret}} \circ d)(a(sb))$ realises $\Downarrow^*(P(x))$, that is, $(s'u) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$.

If $u = \mathbf{Right}(w')$ with $w' \mathbf{r} \Downarrow^*(C(x))$, then $s'u = \mathbf{Right}(aw')$. By the side induction hypothesis, $(aw') \mathbf{r} \Downarrow^*(P(x))$. Thus, $(s'u) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$.

From the proof of (6.1) it follows easily that $s'\downarrow u, s'\downarrow v \in (\tau(P) + \mathbf{A}^*(\tau(P)))$. Therefore, it remains to show:

1. For some $k \in \{u, v\}$, $s'\downarrow k \neq \perp$.
2. If $k \in \{u, v\}$ such that $s'\downarrow k \neq \perp$, then $(s'\downarrow k) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$.

For (1) assume without restriction that $k = u \neq \perp$. Then $s'\downarrow u = s'u$. By (6.1), $(s'u) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$. Hence, $s'u \neq \perp$.

To prove (2), suppose $s'\downarrow k \neq \perp$. Then $k \neq \perp$. It follows that $(s'\downarrow k) \mathbf{r}(P(x) \vee \Downarrow^*(P(x)))$, by (6.1). \square

For what follows, we extend CFP again by adding Rule (CAIB*).

7. CONCURRENT SIGNED DIGIT AND GRAY CODES

We first briefly formalise the definitions given in Section 3 in IFP and CFP, respectively. For details the reader is referred to [BT21a, BT21b].

Define the IFP predicates $\mathbf{SD}(x)$ and $\mathbf{S}(x)$ as follows

$$\begin{aligned} \mathbf{SD}(z) &\stackrel{\text{Def}}{=} (z = -1 \vee z = 1) \vee z = 0, \\ \mathbf{II}(z, x) &\stackrel{\text{Def}}{=} |2x - z| \leq 1, \\ \mathbf{S}(x) &\stackrel{\vee}{=} (\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{S}(2x - z). \end{aligned}$$

For $\mathbf{3} \stackrel{\text{Def}}{=} (\mathbf{1} + \mathbf{1}) + \mathbf{1}$ and $\delta^\omega \stackrel{\text{Def}}{=} \mathbf{fix} \alpha. \delta \times \alpha$, their types are

$$\tau(\mathbf{SD}) = \mathbf{3} \quad \text{and} \quad \tau(\mathbf{S}) = \mathbf{3}^\omega.$$

The predicate $\mathbf{SD}(z)$ is realised as follows

$$d \mathbf{r} \mathbf{SD}(z) = (d = \mathbf{Left}(\mathbf{Left}(\mathbf{Nil})) \wedge z = -1) \vee$$

$$(d = \mathbf{Left}(\mathbf{Right}(\mathbf{Nil})) \wedge z = 1) \vee \\ (d = \mathbf{Right}(\mathbf{Nil}) \wedge z = 0).$$

In the sequel the three digits $-1, 1, 0$ will be identified with their realisers, which are programs of type **3**. For the predicate $\mathbf{S}(x)$ we obtain

$$p \mathbf{r} \mathbf{S}(x) \stackrel{\vee}{=} (\exists d, p') p = \mathbf{Pair}(d, p') \wedge (\exists z) d \mathbf{r} \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge p' \mathbf{r} \mathbf{S}(2x - z) \\ \stackrel{\vee}{=} (\exists d, p') p = \mathbf{Pair}(d, p') \wedge \mathbf{II}(d, x) \leq 1 \wedge p' \mathbf{r} \mathbf{S}(2x - d).$$

The realisers of $\mathbf{S}(x)$ are hence streams of digits $-1, 0, 1$.

Let us next consider the Gray code case. Define

$$\mathbf{B}(x) \stackrel{\text{Def}}{=} x \leq 0 \vee x \geq 0, \\ \mathbf{D}(x) \stackrel{\text{Def}}{=} x \neq 0 \rightarrow \mathbf{B}(x), \\ \mathbf{t}(x) \stackrel{\text{Def}}{=} 1 - 2|x|, \\ \mathbf{G}(x) \stackrel{\vee}{=} (-1 \leq x \leq 1) \wedge \mathbf{D}(x) \wedge \mathbf{G}(\mathbf{t}(x)),$$

where types are $\tau(\mathbf{B}) = \tau(\mathbf{D}) = \mathbf{2}$ with $\mathbf{2} \stackrel{\text{Def}}{=} \mathbf{1} + \mathbf{1}$, and $\tau(\mathbf{G}) = \mathbf{2}^\omega$. Then the predicates $\mathbf{D}(x)$ and $\mathbf{G}(x)$ are realised as follows

$$a \mathbf{r} \mathbf{D}(x) = a : \mathbf{2} \wedge (x \neq 0 \rightarrow (a = \mathbf{Left}(\mathbf{Nil}) \wedge x \leq 0) \vee (a = \mathbf{Right}(\mathbf{Nil}) \wedge x \geq 0)), \\ q \mathbf{r} \mathbf{G}(x) \stackrel{\vee}{=} (-1 \leq x \leq 1) \wedge (\exists a, q') q = \mathbf{Pair}(a, q') \wedge a \mathbf{r} \mathbf{D}(x) \wedge q' \mathbf{r} \mathbf{G}(\mathbf{t}(x)).$$

Since an infinite Gray code may contain a \perp , a sequential access of the sequence from left to right will diverge when it accesses a \perp . However, because at most one \perp is contained in each sequence, if one evaluates the first two cells concurrently, then at least one of the two processes is guaranteed to terminate. On the basis of this idea Berger and Tsuiki [BT21b] showed that a concurrent algorithm converting infinite Gray code into signed digit representation can be extracted from a CFP proof. To this end a concurrent variant of the predicate \mathbf{S} is introduced

$$\mathbf{S}_2(x) \stackrel{\vee}{=} \Downarrow((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{S}_2(2x - z)).$$

$\mathbf{S}_2(x)$ means that a signed digit representation of x is obtained through the concurrent computation of two threads. Note that $\tau(\mathbf{S}_2) = \mathbf{fix} \alpha. \mathbf{A}(\mathbf{3} \times \alpha)$.

Theorem 7.1 [BT21b]. $\mathbf{S} \subseteq \mathbf{G} \subseteq \mathbf{S}_2$.

This result expresses the fact that, as explained above, when computably translating from Gray code to signed digit representation one needs to allow for computations to be carried out concurrently, which, however is not the case for the converse translation from signed digit representation to Gray code. On the other hand the result is not completely satisfying, as one would like to see under which conditions both representations are computably equivalent.

To achieve a result of this kind we have to introduce concurrent Gray code. In addition we have to allow for iterated concurrent computations. Define

$$\mathbf{S}^*(x) \stackrel{\vee}{=} \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{S}^*(2x - z)), \\ \mathbf{B}^*(x) \stackrel{\text{Def}}{=} \Downarrow^*(x \leq 0 \vee x \geq 0), \\ \mathbf{D}^*(x) \stackrel{\text{Def}}{=} x \neq 0 \rightarrow \mathbf{B}^*(x),$$

$$\mathbf{G}^*(x) \stackrel{\nu}{=} (-1 \leq x \leq 1) \wedge \mathbf{D}^*(x) \wedge \mathbf{G}^*(\mathbf{t}(x)).$$

For the concurrent signed digit representation we have $\mathbf{S}^* = \nu(\Phi_{\mathbf{S}^*})$ where

$$\begin{aligned} \Phi_{\mathbf{S}^*}(Y)(x) &= \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge Y(2x - z)), \\ \tau(\Phi_{\mathbf{S}^*})(\alpha) &= \mathbf{A}^*(\mathbf{3} \times \alpha), \\ \tau(\mathbf{S}^*) &= \mathbf{fix} \tau(\Phi_{\mathbf{S}^*}) = \mathbf{fix} \alpha . \mathbf{A}^*(\mathbf{3} \times \alpha), \\ \mathbf{mon}_{\tau(\Phi_{\mathbf{S}^*})} : (\alpha \rightarrow \beta) &\rightarrow \mathbf{A}^*(\mathbf{3} \times \alpha) \rightarrow \mathbf{A}^*(\mathbf{3} \times \beta), \\ \mathbf{mon}_{\tau(\Phi_{\mathbf{S}^*})} f &= f_{\mathbf{mon}} (\lambda \mathbf{Pair}(d, a) . \mathbf{Pair}(d, f a)), \end{aligned}$$

and

$$\begin{aligned} \mathbf{A}^*(\alpha) &= \mathbf{fix} \beta . \mathbf{A}(\alpha + \beta), \\ f_{\mathbf{mon}} : (\alpha \rightarrow \beta) &\rightarrow \mathbf{A}^*(\alpha) \rightarrow \mathbf{A}^*(\beta), \\ f_{\mathbf{mon}}^{\mathbf{rec}} &\stackrel{\mathbf{rec}}{=} \lambda h . \mathbf{mapamb} (\lambda d . \mathbf{case} \, d \, \text{of} \, \{\mathbf{Left}(a) \rightarrow \mathbf{Left}(h a); \mathbf{Right}(c) \rightarrow f_{\mathbf{mon}} h c\}). \end{aligned}$$

On the other hand, for the concurrent infinite Gray code we have $\mathbf{G}^* = \nu(\Phi_{\mathbf{G}^*})$ where

$$\begin{aligned} \Phi_{\mathbf{G}^*}(Y)(x) &= \mathbf{D}^*(x) \wedge Y(\mathbf{t}(x)), \\ \tau(\Phi_{\mathbf{G}^*})(\alpha) &= \mathbf{A}^*(\mathbf{2}) \times \alpha, \\ \tau(\mathbf{G}^*) &= \mathbf{fix} \tau(\Phi_{\mathbf{G}^*}) = \mathbf{fix} \alpha . \mathbf{A}^*(\mathbf{2}) \times \alpha = (\mathbf{A}^*(\mathbf{2}))^\omega, \\ \mathbf{mon}_{\tau(\Phi_{\mathbf{G}^*})} : (\alpha \rightarrow \beta) &\rightarrow (\mathbf{A}^*(\mathbf{2}) \times \alpha) \rightarrow (\mathbf{A}^*(\mathbf{2}) \times \beta), \\ \mathbf{mon}_{\tau(\Phi_{\mathbf{G}^*})} f &\mathbf{Pair}(m, a) = \mathbf{Pair}(m, f a). \end{aligned}$$

We see that a realiser of $\mathbf{G}^*(x)$ is simply an ordinary infinite stream (where the cons-operation is the deterministic constructor \mathbf{Pair}) of non-deterministic partial binary digits, whereas a realiser of $\mathbf{S}^*(x)$ is something that could be called a non-deterministic stream (where the cons-operation is non-deterministic) given by a pair of concurrent computations at least one of which will yield a head, which is signed digit, and a tail, which is again a non-deterministic stream. Consequently, the function $\mathbf{mon}_{\tau(\Phi_{\mathbf{G}^*})}$ is much simpler than $\mathbf{mon}_{\tau(\Phi_{\mathbf{S}^*})}$.

Our next goal is to show that $\mathbf{S}^* = \mathbf{G}^*$. Note that iterated concurrent computations also occur in the case of \mathbf{S}_2 , which can be seen by unfolding the co-inductive definition.

Lemma 7.2. *If $\mathbf{S}^*(x)$, then also*

1. $\mathbf{S}^*(-x)$ and
2. $\mathbf{S}^*(\mathbf{t}(x))$.

Proof. (1) Let $P \stackrel{\text{Def}}{=} \{x \mid \mathbf{S}^*(-x)\}$. We use co-induction to prove that $P \subseteq \mathbf{S}^*$. So, we have to show that

$$\mathbf{S}^*(-x) \rightarrow \Downarrow^*((\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', x) \wedge \mathbf{S}^*(-(2x - z'))),$$

i.e.,

$$\Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, -x) \wedge \mathbf{S}^*(-2x - z)) \rightarrow \Downarrow^*((\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', x) \wedge \mathbf{S}^*(-(2x - z'))).$$

Because of Rule (\Downarrow^* -mon) it suffices to prove that

$$(\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, -x) \wedge \mathbf{S}^*(-2x - z) \rightarrow (\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', x) \wedge \mathbf{S}^*(-(2x - z')).$$

Let $z \in \mathbf{SD}$. We show that

$$\mathbf{II}(z, -x) \wedge \mathbf{S}^*(-2x - z) \rightarrow (\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', x) \wedge \mathbf{S}^*(-(2x - z')).$$

If $\mathbf{II}(z, -x)$ with $\mathbf{S}^*(-2x - z)$, then $\mathbf{II}(-z, x)$. Moreover, $\mathbf{S}^*(-(2x - z'))$ with $z' = -z$.

(2) Let $\mathbf{Q} \stackrel{\text{Def}}{=} \{y \mid (\exists x) \mathbf{S}^*(x) \wedge y = \mathbf{t}(x)\}$. We use concurrent half-strong co-induction (Lemma 5.10) to show that $\mathbf{Q} \subseteq \mathbf{S}^*$. This means that we have to prove that

$$\mathbf{Q}(y) \rightarrow \Downarrow^* (\Downarrow^* ((\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', y) \wedge \mathbf{Q}(2y - z'))) \vee \mathbf{S}^*(y).$$

By the definition of \mathbf{Q} we therefore have to show for x, y with $y = \mathbf{t}(x)$ that

$$\Downarrow^* ((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{S}^*(2x - z)) \rightarrow \Downarrow^* (\Downarrow^* ((\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', y) \wedge \mathbf{Q}(2y - z'))) \vee \mathbf{S}^*(y).$$

Because of the monotonicity and return rules for \Downarrow^* , it suffices to prove that for x, y , with $y = \mathbf{t}(x)$ and $z \in \mathbf{SD}$ that

$$\mathbf{II}(z, x) \wedge \mathbf{S}^*(2x - z) \rightarrow ((\exists z') \mathbf{SD}(z') \wedge \mathbf{II}(z', y) \wedge \mathbf{Q}(2y - z')) \vee \mathbf{S}^*(y),$$

which follows by case distinction:

Case $z = -1$ We have that $x \in [-1, 0]$ and $\mathbf{S}^*(2x + 1)$. Since $2x + 1 = \mathbf{t}(x) = y$ in this case, it follows that $\mathbf{S}^*(y)$.

Case $z = 1$ Now, $x \in [0, 1]$. Therefore, $2x - 1 = -\mathbf{t}(x) = -y$. Since moreover, $\mathbf{S}^*(2x - 1)$, we have that $\mathbf{S}^*(-y)$, from which we obtain that $\mathbf{S}^*(y)$, by Part (1).

Case $z = 0$ It follows that $x \in [-1/2, 1/2]$, which implies that $\mathbf{II}(1, \mathbf{t}(x))$. Therefore, it suffices to show that $\mathbf{Q}(2y - 1)$. Note that $2y - 1 = -\mathbf{t}(y) = -\mathbf{t}(\mathbf{t}(x)) = \mathbf{t}(2x)$. Since $\mathbf{S}^*(2x)$, it follows that $\mathbf{Q}(2y - 1)$. \square

The first statement is realised by

$$f_{7.2.1} \stackrel{\text{Def}}{=} f_{\text{mon}} \lambda \mathbf{Pair}(d, a). \mathbf{Pair}(-d, a),$$

and the second by

$$\begin{aligned} f_{7.2.2} \stackrel{\text{Def}}{=} \mathbf{chscoit}_{\tau(\Phi_{\mathbf{S}^*})} (f_{\text{mon}} \lambda \mathbf{Pair}(d, a). \\ \text{case } d \text{ of } \{-1 \rightarrow \mathbf{Right}(a); \\ 1 \rightarrow \mathbf{Right}(f_{7.2.1} a); \\ 0 \rightarrow \mathbf{Left}(\mathbf{Amb}(\mathbf{Left}(\mathbf{Pair}(1, a)), \perp))\}). \end{aligned}$$

Proposition 7.3. $\mathbf{S}^* \subseteq \mathbf{G}^*$.

Proof. The proof is by co-induction. Because of Lemma 7.2(2) it remains to show that

$$\mathbf{S}^*(x) \rightarrow \mathbf{D}^*(x),$$

that is, $(\forall x \in \mathbf{S}^* \setminus \{0\}) \Downarrow^* (\mathbf{B}(x))$. We prove this formula by iterated concurrent Archimedean induction (CAIB^{*}). Therefore, we have to show

$$(\forall x \in \mathbf{S}^* \setminus \{0\}) \Downarrow^* (\mathbf{B}(x) \vee (|x| \leq 1/2 \wedge \mathbf{S}^*(2x) \wedge (\mathbf{B}(2x) \rightarrow \mathbf{B}(x)))).$$

By Rule (\Downarrow^* -mon) and since $\mathbf{B}(2x) \rightarrow \mathbf{B}(x)$ holds, it suffices to show

$$((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{S}^*(2x - d)) \rightarrow (\mathbf{B}(x) \vee (|x| \leq 1/2 \wedge \mathbf{S}^*(2x))).$$

Let $z \in \mathbf{SD}$ with $\mathbf{II}(z, x)$ and $\mathbf{S}^*(2x - z)$. If $z = -1$ or $z = 1$, then $x \leq 0$ or $x \geq 0$, hence $\mathbf{B}(x)$. If $z = 0$, then $|2x| \leq 1$ and $\mathbf{S}^*(2x)$. \square

Statement $\mathbf{S}^* \subseteq \mathbf{D}^*$ is realised by

$$f_d \stackrel{\text{Def}}{=} \mathbf{caibs} (f_{\text{mon}} \lambda \mathbf{Pair}(d, a). \mathbf{case} \, d \, \mathbf{of} \, \{-1 \rightarrow \mathbf{Left}(-1); \\ 1 \rightarrow \mathbf{Left}(1); \\ 0 \rightarrow \mathbf{Right}(\mathbf{Pair}(a, \text{id}))\}),$$

and the inclusion $\mathbf{S}^* \subseteq \mathbf{G}^*$ by $f_{7.3} \stackrel{\text{Def}}{=} \mathbf{coit}_{\tau(\Phi_{\mathbf{G}^*})} (\lambda c. \mathbf{Pair}(f_d c, f_{7.2.2} c))$, that is,

$$f_{7.3} c \stackrel{\text{rec}}{=} \mathbf{Pair}(f_d c, f_{7.3} (f_{7.2.2} c)).$$

Let us now consider the converse inclusion.

Lemma 7.4. $\mathbf{G}^*(x) \rightarrow \mathbf{G}^*(-x)$.

Proof. Let $\mathbf{P} \stackrel{\text{Def}}{=} \{x \mid \mathbf{G}^*(-x)\}$. We will use strong co-induction to show that $\mathbf{P} \subseteq \mathbf{G}^*$. To this end it needs to be shown that

$$\mathbf{P}(y) \rightarrow \mathbf{D}^*(y) \wedge (\mathbf{P}(\mathbf{t}(y)) \vee \mathbf{G}^*(\mathbf{t}(y))).$$

Assume that $\mathbf{P}(y)$. Then $y = -x$ for some $x \in \mathbf{G}^*$. It follows that $\mathbf{D}^*(x)$ and $\mathbf{G}^*(\mathbf{t}(x))$. The first property implies that $\mathbf{D}^*(-x)$, that is $\mathbf{D}^*(y)$. Moreover, since $\mathbf{t}(x) = \mathbf{t}(-x)$, we also have $\mathbf{G}^*(\mathbf{t}(y))$. \square

The statement $(\forall x) (\mathbf{G}^*(x) \rightarrow \mathbf{G}^*(-x))$ is realised by

$$f_{7.4} \mathbf{Pair}(m, a) \stackrel{\text{Def}}{=} \mathbf{Pair}(f_{\text{mon}} (\lambda d. -d) m, a).$$

Lemma 7.5. For $d \in \{-1, 1\}$,

$$\mathbf{G}^*(x) \rightarrow \mathbf{II}(d, x) \rightarrow \mathbf{G}^*(2x - d).$$

Proof. By case distinction on d we show that

$$\mathbf{G}^*(x) \rightarrow \mathbf{G}^*(2x - d).$$

Therefore, assume that $\mathbf{G}^*(x)$. Then $\mathbf{D}^*(x)$ and $\mathbf{G}^*(\mathbf{t}(x))$.

Case $d = -1$. This case is obvious as $\mathbf{t}(x) = 2x + 1$.

Case $d = 1$. Now $\mathbf{t}(x) = 1 - 2x = -(2x - 1)$. Therefore, the statement follows with Lemma 7.4. \square

$(\forall x) (\mathbf{G}^*(x) \rightarrow (\forall d \in \{-1, 1\}) (\mathbf{II}(d, x) \rightarrow \mathbf{G}^*(2x - d)))$ is realised by

$$f_{7.5} \mathbf{Pair}(-, a) d \stackrel{\text{Def}}{=} \mathbf{case} \, d \, \mathbf{of} \, \{-1 \rightarrow a; 1 \rightarrow f_{7.4} a\}.$$

Lemma 7.6. $\mathbf{II}(1, x) \wedge \mathbf{G}^*(x) \rightarrow \mathbf{G}^*(1 - x)$.

Proof. Assume $\mathbf{II}(1, x)$ and $\mathbf{G}^*(x)$. $\mathbf{II}(1, x)$ implies $\mathbf{II}(1, 1 - x)$ and hence $\mathbf{D}^*(1 - x)$. Therefore, it suffices to show $\mathbf{G}^*(\mathbf{t}(1 - x))$. Note that in our case, $\mathbf{t}(1 - x) = 2x - 1$. Thus, $\mathbf{G}^*(x)$ implies $\mathbf{G}^*(\mathbf{t}(1 - x))$, by Lemma 7.5. \square

$(\forall x) (\mathbf{II}(1, x) \wedge \mathbf{G}^*(x) \rightarrow \mathbf{G}^*(1 - x))$ is realised by

$$f_{7.6} a \stackrel{\text{Def}}{=} \mathbf{Pair}(\mathbf{Amb}(\mathbf{Left}(1), \perp), f_{7.5} a 1).$$

Hence,

$$f_{7.6} \mathbf{Pair}(_, a) = \mathbf{Pair}(\mathbf{Amb}(\mathbf{Left}(1), \perp), f_{7.4} a).$$

Lemma 7.7. $\mathbf{II}(0, x) \wedge \mathbf{G}^*(x) \rightarrow \mathbf{G}^*(2x)$.

Proof. Assume $\mathbf{II}(0, x)$ and $\mathbf{G}^*(x)$. Then $\mathbf{D}^*(x)$ and $\mathbf{G}^*(\mathbf{t}(x))$. Hence also $\mathbf{D}^*(2x)$ and $\mathbf{t}(x) \geq 0$. With Lemma 7.6 it follows $\mathbf{G}^*(2|x|)$ (since $1 - \mathbf{t}(x) = 2|x|$). Therefore, $\mathbf{G}^*(\mathbf{t}(2x))$ (since $\mathbf{t}(|x|) = \mathbf{t}(x)$). It follows $\mathbf{G}^*(2x)$. \square

$(\forall x) (\mathbf{II}(0, x) \wedge \mathbf{G}^*(x) \rightarrow \mathbf{G}^*(2x))$ is realised by

$$f_{7.7} \mathbf{Pair}(m, a) \stackrel{\text{Def}}{=} \mathbf{Pair}(m, \pi_R(f_{7.6} a)).$$

Lemma 7.8. $\mathbf{D}^*(x) \leftrightarrow \Downarrow^*(x \leq 0 \vee x \geq 0) \upharpoonright_{x \neq 0}$.

Proof. Note that $\neg(x \neq 0)$, i.e. $x = 0$, implies that $x \leq 0 \wedge x \geq 0$. Now, assume that $\mathbf{D}^*(x)$. Then we obtain with Rule ($\Downarrow^* \upharpoonright$ -intro) that $\Downarrow^*(x \leq 0 \vee x \geq 0) \upharpoonright_{x \neq 0}$.

For the converse implication assume that $x \neq 0$. Then it follows with Rule (\upharpoonright -mp) that $\Downarrow^*(x \leq 0 \vee x \geq 0)$. So, $\mathbf{D}^*(x)$ holds. \square

$(\forall x) (\mathbf{D}^*(x) \rightarrow \Downarrow^*(x \leq 0 \vee x \geq 0) \upharpoonright_{x \neq 0})$ is realised by the function h^+ as defined in Lemma 5.6. The converse implication is realised by the identity.

Lemma 7.9. $\mathbf{G}^*(x) \rightarrow \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x))$.

Proof. Assume $\mathbf{G}^*(x)$. We have to show $A(x) \stackrel{\text{Def}}{=} \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x))$. By Rule ($\Downarrow^* \upharpoonright$ -absorb), it suffices to show $\Downarrow(A(x))$. Therefore, by Rule ($\Downarrow^* \vee$ -elim) it is sufficient to derive

1. $A(x) \upharpoonright_{x \neq 0}$
2. $A(x) \upharpoonright_{\mathbf{t}(x) \neq 0}$.

Set $\mathbf{D}'(y) \stackrel{\text{Def}}{=} \Downarrow^*(y \leq 0 \vee y \geq 0) \upharpoonright_{\mathbf{t}(y) \neq 0}$. The assumption $\mathbf{G}^*(x)$ entails $\mathbf{D}^*(x)$ and $\mathbf{D}^*(\mathbf{t}(x))$ and therefore also $\mathbf{D}'(x)$ as well as $\mathbf{D}'(\mathbf{t}(x))$, by Lemma 7.8. Now, (1) follows immediately from $\mathbf{D}'(x)$, by Rules ($\Downarrow^* \text{-mon}$) and (\upharpoonright -mon).

For (2) we use that $\mathbf{D}'(\mathbf{t}(x))$. Because of Rule (\upharpoonright -mon) it suffices to derive $\Downarrow^*(\mathbf{t}(x) \leq 0 \vee \mathbf{t}(x) \geq 0) \rightarrow A(x)$. With Rule ($\Downarrow^* \text{-bind}$) this can be further reduced to showing $(\mathbf{t}(x) \leq 0 \vee \mathbf{t}(x) \geq 0) \rightarrow A(x)$. If $\mathbf{t}(x) \leq 0$, then $x \neq 0$, and hence $\Downarrow^*(x \leq 0 \vee x \geq 0)$ because of $\mathbf{D}^*(x)$. As $x \leq 0 \vee x \geq 0 \rightarrow (\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x)$, an application of Rule ($\Downarrow^* \text{-mon}$) leads to $A(x)$. If $\mathbf{t}(x) \geq 0$, then $\mathbf{II}(0, x)$. Hence, $A(x)$, by Rule ($\Downarrow^* \text{-return}$). \square

$(\forall x) (\mathbf{G}^*(x) \rightarrow \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x)))$ is realised by the function

$$f_{7.9} \mathbf{Pair}(m, \mathbf{Pair}(n, _)) \stackrel{\text{Def}}{=} \mathbf{mapamb} \mathbf{Right} \mathbf{Amb}(h^+ m, \\ f_{\text{bind}}(\lambda c. \mathbf{case} \ c \ \mathbf{of} \ \{\mathbf{Left}(a) \rightarrow m; \mathbf{Right}(b) \rightarrow f_{\text{ret}} 0\}) n).$$

Proposition 7.10. $\mathbf{G}^* \subseteq \mathbf{S}^*$.

Proof. Again the assertion follows by co-induction. We have to show that

$$\mathbf{G}^*(x) \rightarrow \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{G}^*(2x - z)).$$

From Lemmas 7.5 and 7.7 it follows

$$\mathbf{G}^*(x) \rightarrow (\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x) \rightarrow (\exists z) (\mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{G}^*(2x - z)),$$

from which we obtain by Rule (\Downarrow -*mon*) that

$$\mathbf{G}^*(x) \rightarrow \Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x)) \rightarrow \Downarrow^*((\exists z) (\mathbf{SD}(z) \wedge \mathbf{II}(z, x) \wedge \mathbf{G}^*(2x - z))).$$

Note that because of Lemma 7.9 the assumption $\Downarrow^*((\exists z) \mathbf{SD}(z) \wedge \mathbf{II}(z, x))$ can be discharged. \square

The inclusion $\mathbf{G}^* \subseteq \mathbf{S}^*$ is realised by

$$f_{7.10} \stackrel{\text{Def}}{=} \mathbf{coit}_{\tau(\Phi_{\mathbf{S}^*})} (\lambda a. f_{\text{mon}} (\lambda d. \mathbf{case } d \mathbf{ of } \{-1 \rightarrow f_{7.5} a d; \\ 1 \rightarrow f_{7.5} a d; 0 \rightarrow f_{7.7} a\}) (f_{7.9} a)).$$

Theorem 7.11. $\mathbf{S}^* = \mathbf{G}^*$

8. THE COMPACT SETS CASE

As is well known, the collection $\mathcal{K}(X)$ of non-empty compact subsets of a non-empty compact metric space is a compact space again with respect to the Hausdorff metric μ_H .

Definition 8.1. Let (X, E) be a digit space. A *digital tree* is a nonempty set $T \subseteq E^{<\omega}$ of finite sequences of digits that is downwards closed under the prefix ordering and has no maximal element, that is, $[] \in T$ and whenever $[e_0, \dots, e_n] \in T$, then $[e_0, \dots, e_{n-1}] \in T$ and $[e_0, \dots, e_n, e] \in T$ for some $e \in E$.

Let \mathcal{T}_E denote the set of digital trees with digits in E . Note that each such tree is finitely branching as E is finite. Moreover, every element $[e_0, \dots, e_{n-1}] \in T$ can be continued to an infinite path α in T , that is, $\alpha \in E^\omega$ is such that $\alpha_i = e_i$, for $i < n$, and $[\alpha_0, \dots, \alpha_{k-1}] \in T$ for all $k \in \mathbb{N}$. In the following we write $\alpha \in [T]$ to mean that α is a path in T , and by a path we always mean an infinite path. $[T]$ is a non-empty compact subset of E^ω , for every tree $T \in \mathcal{T}_E$, and conversely, for every non-empty compact subset C of E^ω , $C = [T^C]$, where $T^C \stackrel{\text{Def}}{=} \{\alpha^{<n} \mid \alpha \in C \wedge n \in \mathbb{N}\}$ (cf. [BS16]).

For $T \in \mathcal{T}_E$ and $n \geq 0$, let $T^{\leq n}$ be the finite initial subtree of T of height n . Then

$$T^{\leq n} = \{\alpha^{<m} \mid \alpha \in [T] \wedge m \leq n\}.$$

Every such initial subtree defines a map $f_{T,n}: X \rightarrow \mathcal{P}(X)$ from X into the powerset of X in the obvious way:

$$f_{T,n}(x) \stackrel{\text{Def}}{=} \{\vec{e}(x) \mid \vec{e} \in E^n \cap T\}.$$

Definition 8.2. For every $T \in \mathcal{T}_E$ we define its *value* by

$$\Downarrow(T) \stackrel{\text{Def}}{=} \bigcap_{n \in \mathbb{N}} f_{T,n}[X].$$

Lemma 8.3 [BS16]. $\langle T \rangle = \{ \llbracket \alpha \rrbracket \mid \alpha \in [T] \}$.

The metric defined on E^ω in Section 2 can be transferred to \mathcal{T}_E . As we will see next, it coincides with the Hausdorff metric.

Lemma 8.4 [BS16]. For $S, T \in \mathcal{T}_E$,

$$\delta_H(S, T) = \begin{cases} 0 & \text{if } S = T, \\ 2^{-\min\{n \mid S^{\leq n} \neq T^{\leq n}\}} & \text{otherwise.} \end{cases}$$

Proposition 8.5 [BS16].

1. $\langle \cdot \rangle: \mathcal{T}_E \rightarrow \mathcal{K}(X)$ is onto and uniformly continuous.
2. The topology on $\mathcal{K}(X)$ induced by the Hausdorff metric is equivalent to the quotient topology induced by $\langle \cdot \rangle$.

As a consequence of Lemma 8.3 we have for trees $T_1, T_2 \in \mathcal{T}_E$ that

$$\langle T_1 \rangle = \langle T_2 \rangle \iff (\forall \alpha \in [T_1])(\exists \beta \in [T_2]) \alpha \sim \beta \wedge (\forall \beta \in [T_2])(\exists \alpha \in [T_1]) \alpha \sim \beta.$$

Definition 8.6. A digital tree $T \in \mathcal{T}_E$ is *full*, if $[T]$ is closed under \sim .

Lemma 8.7. Let $T_1, T_2 \in \mathcal{T}_E$ be full. Then

$$\langle T_1 \rangle = \langle T_2 \rangle \iff T_1 = T_2.$$

Proof. We have that

$$\begin{aligned} \langle T_1 \rangle = \langle T_2 \rangle &\Rightarrow (\forall \alpha \in [T_1])(\exists \beta \in [T_2]) \alpha \sim \beta \wedge (\forall \beta \in [T_2])(\exists \alpha \in [T_1]) \alpha \sim \beta \\ &\Rightarrow [T_1] \subseteq [T_2] \wedge [T_2] \subseteq [T_1] \quad (\text{as } T_1, T_2 \text{ are full}) \\ &\Rightarrow T_1 = T_2. \end{aligned}$$

The converse implication holds trivially, as $\langle \cdot \rangle$ is a map. □

Lemma 8.8. Let $T \in \mathcal{T}_E$ and C be a non-empty compact subset of E^ω . Then the following two statements hold:

1. If T is full, then $[T]$ is a non-empty compact subset of E^ω that is closed under \sim .
2. If C is closed under \sim , then T^C is full.

By Proposition 2.4, $\widehat{[\cdot]}$ is a bijection between E^ω / \sim and space X . So, if C is a non-empty compact, and hence closed, subset of X , $\widehat{[\cdot]}^{-1}[C]$ is a non-empty closed subset of E^ω / \sim . Consequently, $\overline{C} \stackrel{\text{Def}}{=} q_{\sim}^{-1}[\widehat{[\cdot]}^{-1}[C]]$ is a non-empty closed, and thus compact, subset of E^ω , which in addition is closed under \sim . It follows that $T^{\overline{C}}$ is a full tree in \mathcal{T}_D with $\llbracket T^{\overline{C}} \rrbracket = C$.

Let \mathcal{T}_E^f be the subspace of full trees in \mathcal{T}_E .

Proposition 8.9. $\langle \cdot \rangle: \mathcal{T}_E^f \rightarrow \mathcal{K}(X)$ is one-to-one and onto.

This shows that $\mathcal{K}(X)$ can be represented in straightforward one-to-one way without requiring that X is represented in this way. For the special case of the real interval \mathbb{I} and Gray code we have seen in Section 2 that $\llbracket \cdot \rrbracket: \widehat{G} \rightarrow \mathbb{I}$ is one-to-one. Hence, every digital tree $T \in \mathcal{T}_{\widehat{GF}}$ with $[T] \subseteq \widehat{G}$ is full.

9. ARCHIMEDEAN INDUCTION FOR COMPACT SETS

Archimedean induction is a formulation of the Archimedean property as an induction principle introduced in [BT21a]. It turned out quite a powerful proof tool. We will now lift this induction principle to the case of non-empty compact sets. Let $\mathbf{Z}(x)$ be the predicate stating that x is an integer. Moreover, for $K : \mathcal{P}(\iota)$ and $n \in \mathbf{Z}$ define

$$\begin{aligned} K \leq 0 &\stackrel{\text{Def}}{=} (\forall x \varepsilon K) x \leq 0, \\ K \geq 0 &\stackrel{\text{Def}}{=} (\forall x \varepsilon K) x \geq 0, \\ |K| &\stackrel{\text{Def}}{=} \{y \mid (\exists x \varepsilon K) y = |x|\}, \\ nK &\stackrel{\text{Def}}{=} \{y \mid (\exists x \varepsilon K) y = nx\}, \\ \mathbf{K}_0(K) &\stackrel{\text{Def}}{=} \mathbf{K}(K) \wedge 0 \notin K. \end{aligned}$$

Here, \mathbf{K} is a predicate constant denoting the set of non-empty compact subsets of the compact interval $\mathbf{I} \stackrel{\text{Def}}{=} [-1, 1]$ (see Section 4.1).

Definition 9.1. *Archimedean induction for compact sets* is the following rule

$$\frac{(\forall K \in \mathbf{K}_0) ((\forall K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \rightarrow P(2K')) \rightarrow P(K))}{(\forall K \in \mathbf{K}_0) P(K)} \text{ (AIC)}.$$

Also Archimedean induction for compact sets is a special case of well-founded induction. Set

$$K'' \prec K \stackrel{\text{Def}}{=} K \in \mathbf{K} \wedge (\exists K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \wedge K'' = 2K').$$

Then the premise of Rule (AIC) is equivalent to $\mathbf{Prog}_{\prec, \mathbf{K}_0}(P)$.

Lemma 9.2. $\mathbf{Acc}_{\prec}(K)$ if and only if $K \in \mathbf{K}_0$.

Proof. The ‘only if’ part follows by induction on $\mathbf{Acc}_{\prec}(K)$. Since $\mathbf{Acc}_{\prec} = \mu\Phi$ with

$$\Phi(X) \stackrel{\text{Def}}{=} \{K \in \mathbf{K} \mid (\forall K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \rightarrow X(2K'))\}$$

we have to show that $\Phi(\mathbf{K}_0) \subseteq \mathbf{K}_0$. Let $K \in \Phi(\mathbf{K}_0)$ and suppose that $0 \varepsilon K$. Then the compact set $\{0\}$ is a subset of K and $|\{0\}| \leq 1/2$. Since $K \in \Phi(\mathbf{K}_0)$, it follows that $2\{0\} \in \mathbf{K}_0$, which is a contradiction.

The ‘if’ part reduces, by \mathbf{BT}_{nc} , to the implication $K \in \mathbf{K}_0 \rightarrow \neg \mathbf{Path}_{\prec}(K)$. Therefore, we assume $K \in \mathbf{K}_0$ and $\mathbf{Path}_{\prec}(K)$ with the aim to arrive at a contradiction. Recall that

$$\mathbf{Path}_{\prec}(K) \stackrel{\nu}{=} K \in \mathbf{K} \wedge (\exists K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \wedge \mathbf{Path}_{\prec}(2K')).$$

Hence by unfolding $\mathbf{Path}_{\prec}(K)$ we can construct a decreasing sequence $(K_n)_{n \in \mathbf{N}} \subseteq \mathbf{K}$ such that $K_0 = K$ and for all $n \in \mathbf{N}$, $|K_n| \leq 2^{-n}$.

The sequence $(K_n)_{n \in \mathbf{N}}$ is constructed such that $K_0 = K$ and for all n , $\mathbf{Path}_{\prec}(2^n K_n)$, $|K_n| \leq 2^{-n}$, and $K_{n+1} \subseteq K_n$. For K_0 the properties hold by assumption. For the step, we use that $\mathbf{Path}_{\prec}(2^n K_n)$ holds and therefore exists $K' \in \mathbf{K}$ such that $K' \subseteq 2^n K_n$, $|K'| \leq 1/2$ and $\mathbf{Path}_{\prec}(2K')$. We set $K_{n+1} \stackrel{\text{Def}}{=} 2^{-n} K'$. Since $2^{n+1} K_{n+1} = 2K'$ it follows that $\mathbf{Path}_{\prec}(2^{n+1} K_{n+1})$ holds. Furthermore, $|K_{n+1}| = 2^{-n} |K'| \leq 2^{-(n+1)}$. Finally, $K_{n+1} = 2^{-n} K' \subseteq 2^{-n} (2^n K_n) = K_n$.

Since K is compact, there exists $x \varepsilon \bigcap_{n \in \mathbf{N}} K_n$. Then $|x| \leq 2^{-n}$, for all $n \in \mathbf{N}$. By the Archimedean axiom, $x = 0$, hence $0 \varepsilon K$, contradicting our assumption. \square

Proposition 9.3. *Archimedean induction for compact sets (AIC) is derivable in $\text{IFP}(\mathcal{A}_R)$ and realised by rec .*

Proof. It remains to show the second statement. Note that both \prec and the predicate $\mathbf{K}_0(K)$ are Harrop. Moreover, let s realise the premise of Rule (AIC). Then s also realises $\mathbf{Prog}_{\prec, \mathbf{K}_0}$. Therefore, it follows with the result in Example 4.8 that $\text{rec } s$ realises $\mathbf{Acc}_{\prec} \cap \mathbf{K}_0 \subseteq P$ which is equivalent to the conclusion of the rule. \square

In applications, Archimedean induction is mostly used for compact sets that are generated in a particular way and therefore come with a special kind of realisers. Here, we are interested in the case that non-empty compact sets are represented by signed digit code.

Definition 9.4. We define the analogue of the signed digit representation for compact sets as

$$\mathbf{S}_{\mathbf{K}}(K) \stackrel{\text{Def}}{=} \mathbf{K}(K) \wedge (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) K \subseteq \mathbf{I}_E \wedge (\forall d \varepsilon E)(K_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d]))$$

with $\mathbf{I}_d \stackrel{\text{Def}}{=} \{x \mid \mathbf{I}(d, x)\}$, $\mathbf{I}_E \stackrel{\text{Def}}{=} \{x \mid (\exists d \varepsilon E) \mathbf{I}(d, x)\}$, $K_d \stackrel{\text{Def}}{=} K \cap \mathbf{I}_d$, and $\mathbf{av}_d(x) \stackrel{\text{Def}}{=} (x + d)/2$.

As follows from the definition of realisability, the type $\tau(\mathbf{S}_{\mathbf{K}}(K))$ of realisers of the formula $\mathbf{S}_{\mathbf{K}}(K)$ is given by

$$\begin{aligned} \tau(\mathbf{S}_{\mathbf{K}}(K)) &= \mathbf{fix} \alpha. \sum_{E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})} \alpha^{\|\mathbf{I}_E\|} \\ &= \mathbf{fix} \alpha. \{-1\} \times \alpha + \{0\} \times \alpha + \{1\} \times \alpha + \{-1, 0\} \times \alpha^2 + \\ &\quad \{-1, 1\} \times \alpha^2 + \{0, 1\} \times \alpha^2 + \{-1, 0, 1\} \times \alpha^3, \end{aligned}$$

which is essentially the set $\mathcal{T}_{\mathbf{SD}}$ of all digital trees.

In the case of non-empty compact sets with property $\mathbf{S}_{\mathbf{K}}$ the Archimedean induction rule can be much simplified. Let $\mathbf{S}_{\mathbf{K}}^0$ denote the set of all $K \in \mathbf{S}_{\mathbf{K}}$ with $0 \notin K$.

Definition 9.5. *Archimedean induction for signed-digit represented compact sets* is the rule

$$\frac{(\forall K \in \mathbf{S}_{\mathbf{K}}^0)(P(K) \vee (\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K))))}{(\forall K \in \mathbf{S}_{\mathbf{K}}^0) P(K)} \quad (\text{AICSD})$$

where P is a non-Harrop predicate.

Proposition 9.6. *Archimedean induction for signed-digit represented compact sets (AICSD) is derivable in $\text{IFP}(\mathcal{A}_R)$, and if s realises the premise, then*

$$f a \stackrel{\text{rec}}{=} \mathbf{case} \ s a \ \mathbf{of} \ \{\mathbf{Left}(b) \rightarrow b; \mathbf{Right}(\mathbf{Pair}(a', h)) \rightarrow h(f a')\}$$

realises the conclusion.

Proof. We will show that Rule (AICSD) is a consequence of Rule (AIC). Set $A(X) \stackrel{\text{Def}}{=} \mathbf{S}_{\mathbf{K}}(X) \rightarrow P(X)$. It suffices to show that the premise of (AICSD) implies the premise of (AIC). Therefore, let $K \in \mathbf{K}_0$ and assume that

$$(\forall K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \rightarrow A(2K')) \quad (9.1)$$

We have to prove that $A(K)$. So, let $K \in \mathbf{S}_{\mathbf{K}}$. Then we need to derive $P(K)$.

By the premise of (AICSD) we have that

1. $P(K)$ or
2. $\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K))$.

In the first case we are done. Let us therefore consider the second case.

Since $|K_0| \leq 1/2$, by (9.1), $A(2(K_0))$ holds, i.e.,

$$\mathbf{S}_{\mathbf{K}}(2(K_0)) \rightarrow P(2(K_0)).$$

Since we know that $\mathbf{S}_{\mathbf{K}}(2(K_0))$, we obtain that $P(2(K_0))$ and hence, as we are considering the second case, that $P(K)$.

As we have just seen, the premise of (AICSD) implies the premise of (AIC). If the first premise is realised by s the latter is realised by

$$s' = \lambda f. \lambda a. \mathbf{case} \ s \ a \ \mathbf{of} \ \{\mathbf{Left}(b) \rightarrow b; \mathbf{Right}(\mathbf{Pair}(a', h)) \rightarrow h(f \ a')\}.$$

Thus, $f \stackrel{\text{rec}}{=} s' f$, i.e.,

$$f \ a \stackrel{\text{rec}}{=} \mathbf{case} \ s \ a \ \mathbf{of} \ \{\mathbf{Left}(b) \rightarrow b; \mathbf{Right}(\mathbf{Pair}(a', h)) \rightarrow h(f \ a')\},$$

realises the conclusion $(\forall K \in \mathbf{S}_{\mathbf{K}}^0) P(K)$. \square

If one strengthens the premise of Rule (AICSD) to all $K \in \mathbf{S}_{\mathbf{K}}$ instead of only those not containing 0, one can strengthen the conclusion to a restriction.

Definition 9.7. *Archimedean induction with restriction for signed-digit represented compact sets* is the rule

$$\frac{(\forall K \in \mathbf{S}_{\mathbf{K}}) (P(K) \vee (\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K))))}{(\forall K \in \mathbf{S}_{\mathbf{K}}) P(K) \upharpoonright_{0 \neq K}} \text{ (AICR)}$$

where P is a productive non-Harrop predicate.

Proposition 9.8. *Archimedean induction with restriction for signed-digit represented compact sets (AICR) is realisable. More precisely, if s realises the premise, then the conclusion is realised by*

$$\chi \ a \stackrel{\text{rec}}{=} \mathbf{case} \ s \ a \ \mathbf{of} \ \{\mathbf{Left}(b) \rightarrow b; \mathbf{Right}(\mathbf{Pair}(a', f)) \rightarrow f \downarrow (\chi \ a')\}.$$

Proof. Assuming $a \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(K)$ we have to show

1. $0 \notin K \rightarrow \chi \ a \neq \perp$
2. $\chi \ a \neq \perp \rightarrow (\chi \ a) \ \mathbf{r} \ P(K)$.

(1) It suffices to show

$$(\forall K \in \mathbf{K}_0)(\forall a) (a \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(K) \rightarrow \chi \ a \neq \perp).$$

We prove the statement by Archimedean induction for compact sets. Let $K \in \mathbf{K}_0$ and assume, as induction hypothesis,

$$(\forall K' \in \mathbf{K})(K' \subseteq K \wedge |K'| \leq 1/2 \rightarrow (\forall a')(a' \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(2K') \rightarrow \chi \ a' \neq \perp)).$$

We need to show that $(\forall a)(a \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(K) \rightarrow \chi \ a \neq \perp)$. Assume $a \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(K)$. Then

$$(s \ a) \ \mathbf{r} \ (P(K) \vee (\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K)))).$$

If $s \ a = \mathbf{Left}(b)$ where $b \ \mathbf{r} \ P(K)$, then $\chi \ a = b$. Since $P(K)$ is productive, by assumption, $b \neq \perp$. Hence, $\chi \ a \neq \perp$. If, however, $s \ a = \mathbf{Right}(\mathbf{Pair}(a', f))$, then $a' \ \mathbf{r} \ \mathbf{S}_{\mathbf{K}}(2(K_0))$ (with $K_0 \in \mathbf{K}$) and $f \ \mathbf{r} \ (P(2(K_0)) \rightarrow P(K))$. Since $|K_0| \leq 1/2$, we have $\chi \ a' \neq \perp$, by the induction hypothesis. It follows that $\chi \ a = f \downarrow (\chi \ a') \neq \perp$. Thus, we are done.

(2) We use Scott induction, that is, we consider the approximations χ_i of χ ,

$$\chi_0 \ a = \perp,$$

$$\chi_{i+1} \ a = \mathbf{case} \ s \ a \ \mathbf{of} \ \{\mathbf{Left}(b) \rightarrow b; \mathbf{Right}(\mathbf{Pair}(a', f)) \rightarrow f \downarrow (\chi_i \ a)\}$$

Observe that a restricted form of Scott induction (as is used here) is included in the axiom set for the extension RIFP of IFP that allows to deal with realisability in a formal way (cf. [BT21a]).

By the continuity of function application, if $\chi a \neq \perp$, then $\chi_i a \neq \perp$, for some $i \in \mathbf{N}$. Therefore, it suffices to show

$$(\forall i \in \mathbf{N})(a \mathbf{r} \mathbf{S}_{\mathbf{K}}(K) \wedge \chi_i a \neq \perp \rightarrow (\chi a) \mathbf{r} P(K)).$$

We induce on i . The induction base is trivial as $\chi_0 a = \perp$. For the induction step assume $a \mathbf{r} \mathbf{S}_{\mathbf{K}}(K)$ and $\chi_{i+1} a \neq \perp$. Then

$$(s a) \mathbf{r} (P(K) \vee (\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K)))).$$

If $s a = \mathbf{Left}(b)$ where $b \mathbf{r} P(K)$, then $\chi a = b$ and we are done. In the other case $s a = \mathbf{Right}(\mathbf{Pair}(a', f))$ where $a' \mathbf{r} \mathbf{S}_{\mathbf{K}}(2(K_0))$ and $f \mathbf{r} (P(2(K_0)) \rightarrow P(K))$. Then $\chi_{i+1} a = f \downarrow (\chi_i a')$. Since $\chi_{i+1} a \neq \perp$ and the application of f is strict, it follows that $\chi_i a' \neq \perp$ as well. By the induction hypothesis we therefore have that $(\chi a') \mathbf{r} P(2(K_0))$. Consequently, $\chi a = (f \downarrow (\chi a')) \mathbf{r} P(K)$. \square

As in the real number case, in what follows also a concurrent version of the predicate $\mathbf{S}_{\mathbf{K}}$ for the signed digit representation of non-empty compact subsets of the interval \mathbf{I} will be considered.

Definition 9.9.

$$\mathbf{S}_{\mathbf{K}}^*(K) \stackrel{\vee}{=} \mathbf{K}(K) \wedge \Downarrow^*((\exists E \in \mathbf{P}_{\mathbf{fin}}(\mathbf{SD})) K \subseteq \mathbf{I}_E \wedge (\forall d \in E)(K_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[K_d]))).$$

In this case the above induction rule is still valid, if we allow the ‘or’ in the premise being decided concurrently.

Definition 9.10. *Concurrent Archimedean induction with restriction for signed-digit represented compact sets* is the following rule

$$\frac{(\forall K \in \mathbf{S}_{\mathbf{K}}^*) \Downarrow (P(K) \vee (\mathbf{S}_{\mathbf{K}}^*(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K))))}{(\forall K \in \mathbf{S}_{\mathbf{K}}^*) P(K) \upharpoonright_{0 \neq K}} \text{ (CAICR)}$$

where $P = \Downarrow^*(P')$ for some non-Harrop predicate P' .

Proposition 9.11. *Concurrent Archimedean induction with restriction for signed-digit represented compact sets (CAICR) is realisable. More precisely, let g be the canonical realiser of Rule (\Downarrow - \Downarrow^* -absorb), namely $g = \mathbf{mapamb} \mathbf{Right}$, and let s realise the premise of (CAICR). Set*

$$s' \stackrel{\text{Def}}{=} \lambda f. \lambda u. \mathbf{case} u \mathbf{of} \{ \mathbf{Left}(u') \rightarrow u'; \mathbf{Right}(\mathbf{Pair}(u'', d)) \rightarrow d \downarrow (f u'') \}.$$

Then the conclusion of (CAICR) is realised by

$$f b \stackrel{\text{rec}}{=} g \downarrow \mathbf{mapamb} (s' f) (s b).$$

Proof. Let $b \mathbf{r} \mathbf{S}_{\mathbf{K}}^*(K)$. We have to show

1. $0 \neq K \rightarrow f b \neq \perp$,
2. $f b \neq \perp \rightarrow (f b) \mathbf{r} P(K)$.

(1) Since $b \mathbf{r} \mathbf{S}_{\mathbf{K}}^*(K)$ it follows that $s b = \mathbf{Amb}(u, v)$ and

$$\begin{aligned} f b &= g \downarrow \mathbf{mapamb} (s' f) (s b) \\ &= g \downarrow \mathbf{Amb}((s' f) \downarrow u, (s' f) \downarrow v) \\ &= \mathbf{Amb}(\mathbf{Right} \downarrow((s' f) \downarrow u), \mathbf{Right} \downarrow((s' f) \downarrow v)) \neq \perp \end{aligned}$$

(2) Again we use Scott induction. For $i \in \mathbb{N}$ let

$$\begin{aligned} f_0 b &\stackrel{\text{Def}}{=} \perp, \\ f_{i+1} b &\stackrel{\text{Def}}{=} g \downarrow \mathbf{mapamb} (s' f_i) (s b). \end{aligned}$$

By the continuity of function application, if $f b \neq \perp$ then $f_i b \neq \perp$, for some $i \in \mathbb{N}$. Therefore, it suffices to show

$$(\forall i \in \mathbb{N}) (b \mathbf{r} \mathbf{S}_{\mathbf{K}}^*(K) \wedge f_i b \neq \perp \rightarrow (f b) \mathbf{r} P(K)).$$

We induce on i . The induction base is trivial as $f_0 b = \perp$. For the induction step assume that $b \mathbf{r} \mathbf{S}_{\mathbf{K}}^*(K)$ and $f_{i+1} b \neq \perp$. As we have seen above, $s b = \mathbf{Amb}(u, v)$. Hence, $f_{i+1} b = \mathbf{Amb}((s' f_i) \downarrow u, (s' f_i) \downarrow v)$. Moreover, $u \neq \perp$ or $v \neq \perp$, and for $k \in \{u, v\}$ with $k \neq \perp$, $(s' f_i) \downarrow k = s' f_i k$ as well as

$$k \mathbf{r} (P(K) \vee (\mathbf{S}_{\mathbf{K}}^*(2(K_0)) \wedge (P(2(K_0)) \rightarrow P(K)))).$$

We show that $(s' f_i k) \mathbf{r} P(K)$.

If $k = \mathbf{Left}(k')$ with $k' \mathbf{r} P(K)$, then $s' f_i k = k'$. Hence we are done. In the other case $k = \mathbf{Right}(\mathbf{Pair}(k'', d))$ where $k'' \mathbf{r} \mathbf{S}_{\mathbf{K}}^*(2(K_0))$ and $d \mathbf{r} (P(2(K_0)) \rightarrow P(K))$. Then $s' f_i k = d \downarrow (f_i k'')$. Since $f_{i+1} b \neq \perp$, we have that also $(s' f_i) \downarrow k \neq \perp$, as otherwise $s' f_i = \perp$ and hence $\mathbf{Amb}((s' f_i) \downarrow u, (s' f_i) \downarrow v) = \perp$ as well as $g \downarrow \mathbf{Amb}((s' f_i) \downarrow u, (s' f_i) \downarrow v) = \perp$. Thus, $d \downarrow (f_i k'') \neq \perp$. Because application is strict, it follows that $f_i k'' \neq \perp$. By the induction hypothesis we therefore have that $(f k'') \mathbf{r} P(2(K_0))$. Hence, $d \downarrow (f k'') \mathbf{r} P(K)$. It follows that $(\mathbf{mapamb} (s' f) (s b)) \mathbf{r} \downarrow \downarrow (P(K))$ and consequently $(f b) \mathbf{r} P(K)$. \square

We extend the rules of CFP by the new Rules (AICR) and (CAICR).

In the following we will use that the elements of $\mathbf{P}_{\text{fin}}(\mathbf{SD})$ are decidable classical subsets of \mathbf{SD} :

Lemma 9.12. *If $E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$, then*

1. $(\forall d \in \mathbf{SD}) (d \varepsilon E \vee d \notin E)$
2. $(\forall d \varepsilon E) \neg \neg (d \in \mathbf{SD})$

Proof. Easy induction on $\mathbf{P}_{\text{fin}}(\mathbf{SD})$. In part (1), \mathbf{SD} could be replaced by any discrete predicate, that is, predicate P such that $(\forall x, y \in P) (x = y \vee x \neq y)$. In part (2), \mathbf{SD} could be replaced by any predicate. \square

Let

$$\mathbf{B}_{\mathbf{K}}(K) \stackrel{\text{Def}}{=} (K \leq 0 \vee K \geq 0) \vee (K_{-1} \neq \emptyset \wedge K_1 \neq \emptyset).$$

Proposition 9.13. *If $\mathbf{S}_{\mathbf{K}}(K)$, then $\mathbf{B}_{\mathbf{K}}(K) \upharpoonright_{0 \neq K}$.*

Proof. It suffices to verify the premise of Rule (AICR) with $P(K) \stackrel{\text{Def}}{=} \mathbf{B}_{\mathbf{K}}(K)$. That is we must show that

$$\mathbf{B}_{\mathbf{K}}(K) \vee (\mathbf{S}_{\mathbf{K}}(2(K_0)) \wedge (\mathbf{B}_{\mathbf{K}}(2(K_0)) \rightarrow \mathbf{B}_{\mathbf{K}}(K))).$$

Since $\mathbf{S}_{\mathbf{K}}(K)$, there is some $E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$ with $K \subseteq \mathbf{I}_E$ so that K_d is non-empty, for all $d \in E$. Thanks to Lemma 9.12 (1), we can do a case analysis on the elements of E .

Case $0 \notin E$, that is, $E \subseteq \mathbf{GC}$. In this case, we have that both K_{-1} and K_1 are not empty, if $E = \mathbf{GC}$; $K \leq 0$, if $1 \notin E$; and $K \geq 0$, if $-1 \notin E$. Hence $\mathbf{B}_{\mathbf{K}}(K)$ holds.

Case $0 \in E$. Then $\mathbf{S}_{\mathbf{K}}(2(K_0))$, by the definition of $\mathbf{S}_{\mathbf{K}}$. It remains to show that $\mathbf{B}_{\mathbf{K}}(2(K_0)) \rightarrow \mathbf{B}_{\mathbf{K}}(K)$. Assume that $\mathbf{B}_{\mathbf{K}}(2(K_0))$. Then also $\mathbf{B}_{\mathbf{K}}(K_0)$.

If both $K_0 \cap \mathbf{I}_{-1}$ and $K_0 \cap \mathbf{I}_1$ are not empty, K_{-1} and K_1 are not empty as well. In case $K_0 \leq 0$, then $K \leq 0$, if, in addition, $1 \notin E$. Otherwise, $K_{-1} \neq \emptyset$ and $K_1 \neq \emptyset$; similarly, if $K_0 \geq 0$. Thus, $\mathbf{B}_{\mathbf{K}}(K)$. \square

10. SIGNED DIGIT AND GRAY CODE FOR NON-EMPTY COMPACT SETS

In this section the Gray code representation of non-empty compact sets is introduced and its connection with the signed digit representation of these sets is studied.

Definition 10.1.

$$\mathbf{G}_{\mathbf{K}}(K) \stackrel{\vee}{=} \mathbf{K}(K) \wedge \mathbf{G}(\mathbf{min} K) \wedge \mathbf{G}(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])).$$

Our first goal is to show that $\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}}$. To this end we need the following results.

Lemma 10.2. *If $\mathbf{S}_{\mathbf{K}}(K)$ then also*

1. $\mathbf{S}_{\mathbf{K}}(-K)$.
2. $\mathbf{S}(\mathbf{min} K)$.
3. $\mathbf{S}(\mathbf{max} K)$.
4. $(\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow \mathbf{S}_{\mathbf{K}}(\mathbf{t}[K_d]))$.

Proof. (1) Let $P \stackrel{\text{Def}}{=} \{K \mid \mathbf{S}_{\mathbf{K}}(-K)\}$. We use co-induction to prove that $P \subseteq \mathbf{S}_{\mathbf{K}}$. That is, we show that

$$P(K) \rightarrow (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge P(\mathbf{av}_d^{-1}[K_d])).$$

Since $\mathbf{S}_{\mathbf{K}}(-K)$, there is some $F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$ so that $-K = \bigcup\{(-K)_d \mid d \in F\}$ and for all $d \in F$, $(-K)_d \neq \emptyset$ as well as $\mathbf{S}_{\mathbf{K}}(\mathbf{av}_d^{-1}[(-K)_d])$. Note that $(-K)_d = -(K_{(-d)})$ and $\mathbf{av}_d^{-1}[(-K)_d] = -\mathbf{av}_{-d}^{-1}[K_{(-d)}]$. Therefore, we can choose $E \stackrel{\text{Def}}{=} \{-d \mid d \in F\}$.

(2) The proof is by co-induction. Let $R \stackrel{\text{Def}}{=} \{x \in \mathbf{I} \mid (\exists K \in \mathbf{S}_{\mathbf{K}}) x = \mathbf{min} K\}$. We show

$$R(x) \rightarrow (\exists d \in \mathbf{SD}) (x \in \mathbf{I}_d \wedge R(\mathbf{av}_d^{-1}(x))).$$

If $x \in R$ then $x = \mathbf{min} K$, for some $K \in \mathbf{S}_{\mathbf{K}}$. Hence, there exists $E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$ so that $K = \bigcup\{K_e \mid e \in E\}$. Moreover, $K_e \neq \emptyset$ and $\mathbf{S}_{\mathbf{K}}(\mathbf{av}_e^{-1}[K_e])$, for all $e \in E$. Order \mathbf{SD} by $-1 < 0 < 1$ and let d be the least element of E with respect to this order (which can be determined, thanks to Lemma 9.12(1)). Then $\mathbf{min} K \in K_d \subseteq \mathbf{I}_d$ and $\mathbf{av}_d^{-1}(\mathbf{min} K) \in \mathbf{av}_d^{-1}[K_d]$. Note that \mathbf{av}_d^{-1} is monotone. Therefore, $\mathbf{av}_d^{-1}(\mathbf{min} K) = \mathbf{min} \mathbf{av}_d^{-1}[K_d]$. Since $\mathbf{av}_d^{-1}[K_d] \in \mathbf{S}_{\mathbf{K}}$, it follows that $\mathbf{av}_d^{-1}(\mathbf{min} K) \in R$.

(3) The statement follows easily with the first two statements and [BT21a, Lemma 23], stating that \mathbf{S} is closed under $\lambda x. -x$,

(4) Let $d \in \mathbf{GC}$ and set

$$Q^d \stackrel{\text{Def}}{=} \{L \mid (\exists K \in \mathbf{S}_{\mathbf{K}}) (K_d \neq \emptyset \wedge L = \mathbf{t}[K_d])\}.$$

We use half-strong co-induction to show that $Q^d \subseteq \mathbf{S}_{\mathbf{K}}$. That is, we prove

$$Q^d(L) \rightarrow ((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (L \subseteq \mathbf{II}_E \wedge (\forall e \in E) (L_e \neq \emptyset \wedge Q^d(\mathbf{av}_e^{-1}[L_e]))) \vee \mathbf{S}_{\mathbf{K}}(L)).$$

Assume that $Q^d(L)$. Then there is some $K \in \mathbf{S}_{\mathbf{K}}$ such that $K_d \neq \emptyset$ and $L = \mathbf{t}[K_d]$. Since $\mathbf{S}_{\mathbf{K}}(K)$, there is some $F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$ so that

- $K \subseteq \mathbf{II}_F$ and
- $(\forall f \in F) (K_f \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}(\mathbf{av}_f^{-1}[K_f]))$.

We perform a case analysis on whether $d \in F$ using Lemma 9.12(1).

If $d \in F$, we have that $\mathbf{S}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d])$. If $d = -1$, then $\mathbf{av}_d^{-1}(x) = 2x + 1 = \mathbf{t}(x)$. Thus, $\mathbf{av}_d^{-1}[K_d] = \mathbf{t}[K_d] = L$. That is, we have that $\mathbf{S}_{\mathbf{K}}(L)$. On the other hand, if $d = 1$, then $\mathbf{av}_d^{-1}(x) = 2x - 1 = -\mathbf{t}(x)$. Hence, $\mathbf{av}_d^{-1}[K_d] = -L$. It follows that $\mathbf{S}_{\mathbf{K}}(-L)$, whence we obtain that $\mathbf{S}_{\mathbf{K}}(L)$.

If $d \notin F$, then $F \subseteq \{0\} \cup \{-d\}$, by Lemma 9.12(2).

Case $0 \in F$. Then $K_d \subseteq \mathbf{II}_0$ and $\mathbf{S}_{\mathbf{K}}(2(K_0))$. Furthermore,

$$2(K_d) = 2(K \cap \mathbf{II}_0 \cap \mathbf{II}_d) = 2(K_0) \cap \mathbf{II}_d$$

and

$$\mathbf{av}_1^{-1}[L] = -\mathbf{t}[L] = -\mathbf{t}[\mathbf{t}[K_d]] = \mathbf{t}[2(K_d)] = \mathbf{t}[2(K_0) \cap \mathbf{II}_d],$$

from which it follows that $Q^d(\mathbf{av}_1^{-1}[L])$. Moreover, $L = \mathbf{t}[K_d] \subseteq \mathbf{t}[\mathbf{II}_0] = \mathbf{II}_1$ and hence $L_1 = L \neq \emptyset$. Therefore, we have proven the left part of the disjunction with $E \stackrel{\text{Def}}{=} \{1\}$.

Case $0 \notin F$. Now, $F = \{-d\}$. Hence $K_d = \{0\}$ and $L = \{1\}$. As it follows by co-induction that $\{\{-1\}, \{1\}\} \subseteq \mathbf{S}_{\mathbf{K}}$, we have $\mathbf{S}_{\mathbf{K}}(L)$. \square

With Theorem 7.1 and Lemma 10.2 we now obtain by co-induction what we were looking for.

Proposition 10.3. $\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}}$.

Remark 10.4. Inspecting the proof of Part (4) of Lemma 10.2, one sees that the extracted realiser yields a defined result for *every* $d \in \mathbf{SD}$, even if $K_d = \emptyset$. In that case the computed realiser of the implication $K_d \neq \emptyset \rightarrow \mathbf{S}_{\mathbf{K}}(\mathbf{t}[K_d])$ is defined but does not necessarily realise $\mathbf{S}_{\mathbf{K}}(\mathbf{t}[K_d])$. Therefore, this implication cannot be strengthened to a restriction. The computation contained in the proof of (4) takes as input only d and F (more precisely, realisers of $d \in \mathbf{SD}$ and $F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$) and a realiser of $\mathbf{S}_{\mathbf{K}}(K)$. It does not use the information that K_d is non-empty. This information is only needed to prove the correctness of the result. Thus the transformation extracted from the proof of Proposition 10.3 outputs for every realiser of $\mathbf{S}_{\mathbf{K}}(K)$ a *total* full binary tree, that is, the addresses of nodes are *all* finite sequences of elements in \mathbf{GC} . Each node $\vec{d} = d_0, \dots, d_{n-1}$ is labelled by a pair of infinite Gray codes such that with $g_{\vec{d}} = [g_{d_0}, \dots, g_{d_{n-1}}]$ (using the notation of Section 2 where g_{-1} and g_1 are the inverses of the legs of \mathbf{t}), if $g_{\vec{d}}^{-1}[K]$ is non-empty, then the label consists of realisers of $\mathbf{G}(\min g_{\vec{d}}^{-1}[K])$ and $\mathbf{G}(\max g_{\vec{d}}^{-1}[K])$. If $g_{\vec{d}}^{-1}[K]$ is empty, the label is meaningless. It is not possible to computationally distinguish meaningful from meaningless labels since in general a realiser of K does not allow us to recognise the non-emptiness of $g_{\vec{d}}^{-1}[K]$. An extreme example is $K = \{0\}$ where we may only ever know that the label at

the root contains reliable information, namely realisers of $\mathbf{G}(\min K)$ and $\mathbf{G}(\max K)$. The labels at all other nodes may never be known to carry correct information. This shows, in particular, that the conjuncts $\mathbf{G}(\min K)$ and $\mathbf{G}(\max K)$, in the co-inductive definition of $\mathbf{G}_{\mathbf{K}}(K)$ cannot be replaced by the weaker formulas $\mathbf{D}(\min K)$ and $\mathbf{D}(\max K)$ which would only provide the first digits of the Gray codes of $\min K$ and $\max K$. If, however, for some node \vec{d} the first digit of the Gray code of $\min g_{\vec{d}}^{-1}[K]$ is defined, it will tell us whether $\min g_{\vec{d}}^{-1}[K] \leq 0$ and hence $(g_{\vec{d}}^{-1}[K])_{-1} \neq \emptyset$, or $\min g_{\vec{d}}^{-1}[K] \geq 0$ and thus $(g_{\vec{d}}^{-1}[K])_1 \neq \emptyset$; similarly for $\max g_{\vec{d}}^{-1}[K]$.

Our next aim is to show that $\mathbf{G}_{\mathbf{K}} \subseteq \mathbf{S}_{\mathbf{K}}^*$. We start with a technical lemma.

Lemma 10.5.

$$\mathbf{G}_{\mathbf{K}}(K) \rightarrow \mathbf{G}_{\mathbf{K}}(-K).$$

Proof. Let $R \stackrel{\text{Def}}{=} \{K \mid \mathbf{G}_{\mathbf{K}}(-K)\}$. We use strong co-induction to show that $R \subseteq \mathbf{G}_{\mathbf{K}}$. That is, we have to show that

$$R(K) \rightarrow (\mathbf{G}(\min K) \wedge \mathbf{G}(\max K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow (R(\mathbf{t}[K_d]) \vee \mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])))).$$

Assume that $R(K)$. Then $\mathbf{G}_{\mathbf{K}}(-K)$ and hence

$$\mathbf{G}(\min(-K)) \wedge \mathbf{G}(\max(-K)) \wedge (\forall d \in \mathbf{GC}) ((-K)_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}(\mathbf{t}[(-K)_d])).$$

Note that $-(K_d) = (-K)_{(-d)}$ and hence $\mathbf{t}[K_d] = \mathbf{t}[(-K)_d] = \mathbf{t}[(-K)_{(-d)}]$. Moreover, $\min(-K) = -\max K$ and $\max(-K) = -\min K$. Since \mathbf{G} is closed under $\lambda x. -x$, by [Be16, Lemma 7], it follows that

$$\mathbf{G}(\max K) \wedge \mathbf{G}(\min K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])),$$

as was to be shown. □

Lemma 10.6. For $d \in \mathbf{GC}$,

$$\mathbf{G}_{\mathbf{K}}(K) \rightarrow K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d]).$$

Proof. The statement follows by case distinction on d . Assume that $\mathbf{G}_{\mathbf{K}}(K)$. Then $\mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])$.

Case $d = -1$. This case is obvious, as for $x \in \mathbf{II}_{-1}$, $\mathbf{t}(x) = 2x + 1 = \mathbf{av}_{-1}^{-1}(x)$.

Case $d = 1$. For $x \in \mathbf{II}_1$, $\mathbf{t}(x) = 1 - 2x = -\mathbf{av}_1^{-1}(x)$. Therefore the statement follows with Lemma 10.5. □

Lemma 10.7. Let $K \subseteq \mathbf{II}_1$. Then

$$\mathbf{G}_{\mathbf{K}}(K) \rightarrow \mathbf{G}_{\mathbf{K}}((\lambda x. 1 - x)[K]).$$

Proof. The statement follows by co-induction. Note to this end that $(\lambda x. 1 - x)[K] \subseteq \mathbf{II}_1$ as well. Moreover, $\min((\lambda x. 1 - x)[K]) = 1 - \max K$ and $\max((\lambda x. 1 - x)[K]) = 1 - \min K$. Now assume that $\mathbf{G}_{\mathbf{K}}(K)$. Then $\mathbf{G}(\min K)$ and $\mathbf{G}(\max K)$. By [Be16, Lemma 10] we have for $x \in \mathbf{II}_1$ with $\mathbf{G}(x)$ that also $\mathbf{G}(1 - x)$. Thus, we obtain $\mathbf{G}(\min(\lambda x. 1 - x)[K])$ and $\mathbf{G}(\max(\lambda x. 1 - x)[K])$. Since for $x \in \mathbf{II}_1$, $\mathbf{t}(1 - x) = 2x - 1 = \mathbf{av}_1^{-1}(x)$, it follows with Lemma 10.6 that $\mathbf{G}_{\mathbf{K}}(\mathbf{t}[(\lambda x. 1 - x)[K]])$. □

Lemma 10.8. Let $K \subseteq \mathbf{II}$. Then

$$\mathbf{G}_{\mathbf{K}}(1/2K) \rightarrow \mathbf{G}_{\mathbf{K}}(K).$$

Proof. The statement follows again by co-induction. Assume that $\mathbf{G}_{\mathbf{K}}(1/2K)$. Then $\mathbf{G}(\mathbf{min} K/2)$ and $\mathbf{G}(\mathbf{max} K/2)$. Since by [Be16, Lemma 11] \mathbf{G} is closed under $\lambda x. 2x$ for $|x| \leq 1/2$, it follows that $\mathbf{G}(\mathbf{min} K)$ and $\mathbf{G}(\mathbf{max} K)$.

As a further consequence of our assumption we have for $d \in \mathbf{GC}$ with $K_d \neq \emptyset$ that $\mathbf{G}_{\mathbf{K}}(\mathbf{t}[1/2K_d])$. Because $\mathbf{t}(x/2) = 1 - |x|$, we obtain that $\mathbf{G}_{\mathbf{K}}((\lambda x. 1 - |x|)[K_d])$. Hence, $\mathbf{G}_{\mathbf{K}}(|K_d|)$, by Lemma 10.7, and therefore $\mathbf{G}_{\mathbf{K}}(\mathbf{t}[K_d])$. \square

Set

$$\begin{aligned} B_0^{\min} &\stackrel{\text{Def}}{=} \mathbf{min} K \neq 0, & B_1^{\min} &\stackrel{\text{Def}}{=} \mathbf{t}(\mathbf{min} K) \neq 0, \\ B_0^{\max} &\stackrel{\text{Def}}{=} \mathbf{max} K \neq 0, & B_1^{\max} &\stackrel{\text{Def}}{=} \mathbf{t}(\mathbf{max} K) \neq 0. \end{aligned}$$

Then

$$\neg\neg(B_0^{\min} \vee B_1^{\min})$$

and

$$\neg\neg(B_0^{\max} \vee B_1^{\max}).$$

It follows for

$$C_{i,j} \stackrel{\text{Def}}{=} B_i^{\min} \wedge B_j^{\max}$$

with $i, j \in \{0, 1\}$ that

$$\neg\neg\left(\bigvee_{0 \leq i, j \leq 1} C_{i,j}\right). \quad (10.1)$$

Moreover, all $C_{i,j}$ are Harrop.

Now, let

$$A(K) \stackrel{\text{Def}}{=} (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset).$$

Lemma 10.9. $\mathbf{G}_{\mathbf{K}}(K) \rightarrow \Downarrow^*(A(K))$.

Proof. Assume $\mathbf{G}_{\mathbf{K}}(K)$. Because of (10.1) and the Rules $(\Downarrow^* \vdash \vee)$, $(\vdash \text{-stab})$, and $(\vdash \text{-mp})$, it suffices to show

1. $A(K) \vdash_{C_{0,0}}$,
2. $A(K) \vdash_{C_{0,1}}$,
3. $A(K) \vdash_{C_{1,0}}$,
4. $A(K) \vdash_{C_{1,1}}$.

The assumption $\mathbf{G}_{\mathbf{K}}(K)$ entails that $\mathbf{G}(\mathbf{min} K)$ and $\mathbf{G}(\mathbf{max} K)$. Hence, we have for $x \in \{\mathbf{min} K, \mathbf{max} K\}$ that

$$(x \geq 0 \vee x \leq 0) \vdash_{x \neq 0}. \quad (10.2)$$

Since from $\mathbf{G}(x)$ we obtain that also $\mathbf{G}(\mathbf{t}(x))$, it follows in the same way that

$$(\mathbf{t}(x) \geq 0 \vee \mathbf{t}(x) \leq 0) \vdash_{\mathbf{t}(x) \neq 0}. \quad (10.3)$$

Note that

$$\begin{aligned} \mathbf{min} K \geq 0 &\leftrightarrow K \geq 0, \\ \mathbf{min} K \leq 0 &\leftrightarrow K_{-1} \neq \emptyset, \\ \mathbf{max} K \leq 0 &\leftrightarrow K \leq 0, \\ \mathbf{max} K \geq 0 &\leftrightarrow K_1 \neq \emptyset. \end{aligned}$$

(1) Observe that $C_{0,0}$ is the formula $(\mathbf{min} K \neq 0 \wedge \mathbf{max} K \neq 0)$. We use (10.2) for $x = \mathbf{min} K$ and $x = \mathbf{max} K$. With Rules ($\vdash\wedge$), ($\vdash\text{-mon}$), and ($\vdash\text{-antimon}$) we then obtain

$$((\mathbf{min} K \geq 0 \vee \mathbf{min} K \leq 0) \wedge (\mathbf{max} K \geq 0 \vee \mathbf{max} K \leq 0)) \vdash_{C_{0,0}} \mathbf{min} K \neq 0 \wedge \mathbf{max} K \neq 0$$

which is equivalent to

$$(\mathbf{min} K \geq 0 \vee (\mathbf{min} K \leq 0 \wedge \mathbf{max} K \geq 0) \vee \mathbf{max} K \leq 0) \vdash_{C_{0,0}}$$

and, by the above equivalences, to

$$(K \geq 0 \vee (K_{-1} \neq \emptyset \wedge K_1 \neq \emptyset) \vee K \leq 0) \vdash_{C_{0,0}}.$$

Since the formula $(K \geq 0 \vee (K_{-1} \neq \emptyset \wedge K_1 \neq \emptyset) \vee K \leq 0)$ clearly implies $A(K)$, we are done by Rule ($\vdash\text{-mon}$).

(2) $C_{0,1}$ is the formula $(\mathbf{min} K \neq 0 \wedge \mathbf{t}(\mathbf{max} K) \neq 0)$. We use (10.2) for $x = \mathbf{min} K$ and (10.3) for $x = \mathbf{max} K$. With a similar argument as in the previous case we receive

$$((\mathbf{min} K \geq 0 \vee \mathbf{min} K \leq 0) \wedge (\mathbf{t}(\mathbf{max} K) \geq 0 \vee \mathbf{t}(\mathbf{max} K) \leq 0)) \vdash_{C_{0,1}}.$$

Therefore, it suffices to show that $A(K)$ is implied by the formula

$$(\mathbf{min} K \geq 0 \vee \mathbf{min} K \leq 0) \wedge (\mathbf{t}(\mathbf{max} K) \geq 0 \vee \mathbf{t}(\mathbf{max} K) \leq 0).$$

The latter is equivalent to

$$(K \geq 0 \vee K_{-1} \neq \emptyset) \wedge (|\mathbf{max} K| \leq 1/2 \vee |\mathbf{max} K| \geq 1/2).$$

If $K \geq 0$, we choose $E \stackrel{\text{Def}}{=} \{1\}$.

If $K_{-1} \neq \emptyset$ and $|\mathbf{max} K| \leq 1/2$ we chose $E \stackrel{\text{Def}}{=} \{-1, 0\}$.

If $K_{-1} \neq \emptyset$ and $|\mathbf{max} K| \geq 1/2$ we have $\mathbf{max} K \neq 0$ and can therefore use (10.2) and Rule ($\vdash\text{-mp}$) to get $\mathbf{max} K \geq 0 \vee \mathbf{max} K \leq 0$, that is, $K_1 \neq \emptyset \vee K \leq 0$.

If $K_1 \neq \emptyset$, we choose $E \stackrel{\text{Def}}{=} \{-1, 1\}$. If $K \leq 0$, we choose $E \stackrel{\text{Def}}{=} \{-1\}$.

(3) is dual to (2).

(4) $C_{1,1}$ is the formula $(\mathbf{t}(\mathbf{min} K) \neq 0 \wedge \mathbf{t}(\mathbf{max} K) \neq 0)$. Using (10.3) for $x = \mathbf{min} K$ and $x = \mathbf{max} K$ we obtain

$$((\mathbf{t}(\mathbf{min} K) \geq 0 \vee \mathbf{t}(\mathbf{min} K) \leq 0) \wedge (\mathbf{t}(\mathbf{max} K) \geq 0 \vee \mathbf{t}(\mathbf{max} K) \leq 0)) \vdash_{C_{1,1}}.$$

Therefore, it suffices to show that $A(K)$ is implied by the formula

$$(\mathbf{t}(\mathbf{min} K) \geq 0 \vee \mathbf{t}(\mathbf{min} K) \leq 0) \wedge (\mathbf{t}(\mathbf{max} K) \geq 0 \vee \mathbf{t}(\mathbf{max} K) \leq 0).$$

The latter is equivalent to

$$(|\mathbf{min} K| \leq 1/2 \vee |\mathbf{min} K| \geq 1/2) \wedge (|\mathbf{max} K| \leq 1/2 \vee |\mathbf{max} K| \geq 1/2).$$

If $|\mathbf{min} K| \leq 1/2$ and $|\mathbf{max} K| \leq 1/2$, we choose $E \stackrel{\text{Def}}{=} \{0\}$.

If $|\mathbf{min} K| \leq 1/2$ and $|\mathbf{max} K| \geq 1/2$, then $\mathbf{max} K \geq 1/2$, hence we choose $E \stackrel{\text{Def}}{=} \{0, 1\}$.

If $|\mathbf{min} K| \geq 1/2$ and $|\mathbf{max} K| \leq 1/2$, then $\mathbf{min} K \leq -1/2$, hence we choose $E \stackrel{\text{Def}}{=} \{-1, 0\}$.

If $|\mathbf{min} K| \geq 1/2$ and $|\mathbf{max} K| \geq 1/2$, then, by (10.3), $(\mathbf{min} K \geq 0 \vee \mathbf{min} K \leq 0) \wedge (\mathbf{max} K \geq 0 \vee \mathbf{max} K \leq 0)$, which, as in case (1), implies $A(K)$. \square

The above statements now allow the derivation of the result we are looking for.

Proposition 10.10.

$$\mathbf{G}_K \subseteq \mathbf{S}_K^*.$$

Proof. The statement follows by co-induction. We have to show that

$$\mathbf{G}_{\mathbf{K}}(K) \rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d])))).$$

From Lemmas 10.6 and 10.8 it follows

$$\begin{aligned} \mathbf{G}_{\mathbf{K}}(K) &\rightarrow ((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset)) \\ &\rightarrow (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d]))). \end{aligned}$$

By the monotonicity of \Downarrow^* we thus obtain

$$\begin{aligned} \mathbf{G}_{\mathbf{K}}(K) &\rightarrow (\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset))) \\ &\rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}(\mathbf{av}_d^{-1}[K_d])))), \end{aligned}$$

where, the assumption $\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset))$ can be discharged by Lemma 10.9. \square

The result we have obtained so far is analogous to the number case.

Theorem 10.11. $\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}} \subseteq \mathbf{S}_{\mathbf{K}}^*$.

Remark 10.12. The definition of $\mathbf{G}_{\mathbf{K}}(K)$ (Definition 10.1) can be simplified to

$$\mathbf{G}_{\mathbf{K}}(K) = \mathbf{K}(K) \wedge \mathbf{G}(\mathbf{min} K) \wedge \mathbf{G}'_{\mathbf{K}}(K)$$

where

$$\mathbf{G}'_{\mathbf{K}}(K) \stackrel{\nu}{=} \mathbf{G}(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow \mathbf{G}'_{\mathbf{K}}(\mathbf{t}[K_d])).$$

This is equivalent to 10.1 since \mathbf{G} is closed under the function \mathbf{t} and for $d \in \mathbf{GC}$ with $K_d \neq \emptyset$, $\mathbf{K}(K)$ implies $\mathbf{K}(\mathbf{t}[K_d])$, and if $d = -1$, then $\mathbf{min} \mathbf{t}[K_d] = \mathbf{t}(\mathbf{min} K)$ while for $d = 1$, $\mathbf{min} \mathbf{t}[K_d] = \mathbf{t}(\mathbf{max} K)$. Although the new definition looks more complicated, it leads to simpler realisers since in each recursion step it refers to \mathbf{G} only once. The definition of $\mathbf{G}_{\mathbf{K}}^*(K)$ in the subsequent Section 11 can be simplified in a similar way.

11. CONCURRENT GRAY CODE FOR NON-EMPTY COMPACT SETS

Next, set

$$\mathbf{G}_{\mathbf{K}}^*(K) \stackrel{\nu}{=} \mathbf{K}(K) \wedge \mathbf{G}^*(\mathbf{min} K) \wedge \mathbf{G}^*(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[K_d])).$$

Our next and final goal is to show that $\mathbf{S}_{\mathbf{K}}^* = \mathbf{G}_{\mathbf{K}}^*$.

Lemma 11.1. *If $\mathbf{S}_{\mathbf{K}}^*(K)$ then also*

1. $\mathbf{S}_{\mathbf{K}}^*(-K)$.
2. $\mathbf{S}_{\mathbf{K}}^*(\mathbf{min} K)$.
3. $\mathbf{S}_{\mathbf{K}}^*(\mathbf{max} K)$.
4. $(\forall d \in \mathbf{GC})(K_d \neq \emptyset \rightarrow \mathbf{S}_{\mathbf{K}}^*(\mathbf{t}[K_d]))$.

Proof. (1) Let $P \stackrel{\text{Def}}{=} \{K \mid \mathbf{S}_{\mathbf{K}}^*(-K)\}$. We use co-induction to prove that $P \subseteq \mathbf{S}_{\mathbf{K}}^*$. That is, we have to show that

$$P(K) \rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge P(\mathbf{av}_d^{-1}[K_d])))).$$

By definition of P it suffices to derive

$$\begin{aligned} & \Downarrow^*((\exists F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (-K \subseteq \mathbf{I}_F \wedge (\forall d \in F) ((-K)_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[(-K)_d]))) \\ & \rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge P(\mathbf{av}_d^{-1}[K_d])))). \end{aligned}$$

Because of the monotonicity rule for \Downarrow^* we thus only have to show that

$$\begin{aligned} & (\exists F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (-K \subseteq \mathbf{I}_F \wedge (\forall d \in F) ((-K)_d \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[(-K)_d]))) \\ & \rightarrow (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge P(\mathbf{av}_d^{-1}[K_d])), \end{aligned}$$

which has been done in the proof of Lemma 10.2(1).

(2) The proof is an adaptation of the proof of Lemma 10.2(2). Let

$$R \stackrel{\text{Def}}{=} \{x \in \mathbf{I} \mid (\exists K \in \mathbf{S}_{\mathbf{K}}^*) x = \mathbf{min} K\}.$$

We have to show that

$$R(K) \rightarrow \Downarrow^*((\exists d \in \mathbf{SD}) (x \in \mathbf{I}_d \wedge R(\mathbf{av}_d^{-1}(x)))).$$

Assume $R(K)$. Then there is some $K \in \mathbf{S}_{\mathbf{K}}^*$ with $x = \mathbf{min} K$. It follows that

$$\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall e \in E) (K_e \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_e^{-1}[K_e])))).$$

Because of the monotonicity law for \Downarrow^* it suffices to prove that

$$\begin{aligned} & (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge (\forall e \in E) (K_e \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_e^{-1}[K_e]))) \rightarrow \\ & (\exists d \in \mathbf{SD}) (x \in \mathbf{I}_d \wedge R(\mathbf{av}_d^{-1}(x))). \end{aligned}$$

Order \mathbf{SD} again by $-1 < 0 < 1$ and let d be the least element of E with respect to this order. Then $\mathbf{min} K \in K_d \subseteq \mathbf{I}_d$ and $\mathbf{av}_d^{-1}(\mathbf{min} K) \in \mathbf{av}_d^{-1}[K_d]$. Note that \mathbf{av}_d^{-1} is monotone. Therefore, $\mathbf{av}_d^{-1}(\mathbf{min} K) = \mathbf{min} \mathbf{av}_d^{-1}[K_d]$. Since $\mathbf{av}_d^{-1}[K_d] \in \mathbf{S}_{\mathbf{K}}^*$, it follows that $\mathbf{av}_d^{-1}(\mathbf{min} K) \in R$.

(3) As in Lemma 10.2, the statement is a direct consequence of Statements 1 and 2 as well as Lemma 7.2(1).

(4) Set

$$R_K^d(K) \stackrel{\text{Def}}{=} \{K \mid (\exists Z \in \mathbf{S}_{\mathbf{K}}^*) (Z_d \neq \emptyset \wedge K = \mathbf{t}[Z_d])\}.$$

We use concurrent half-strong co-induction to show that $R_K^d \subseteq \mathbf{S}_{\mathbf{K}}^*$. That is, we have to prove that

$$\begin{aligned} R_K^d(K) \rightarrow \Downarrow^*(\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{I}_E \wedge \\ (\forall e \in E) (K_e \neq \emptyset \wedge R_K^d(\mathbf{av}_e^{-1}[K_e])))) \vee \mathbf{S}_{\mathbf{K}}^*(K))). \end{aligned} \quad (11.1)$$

If $R_K^d(K)$, there is some $Z \in \mathbf{S}_{\mathbf{K}}^*$ so that $Z_d \neq \emptyset$ and $K = \mathbf{t}[Z_d]$. Since $\mathbf{S}_{\mathbf{K}}^*(Z)$, it follows that

$$\Downarrow^*((\exists F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (Z \subseteq \mathbf{I}_F \wedge (\forall f \in F) (Z_f \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_f^{-1}[Z_f])))).$$

Now, assume that there is some $F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})$ such that $Z = \bigcup_{f \in F} Z_f$ and for all $f \in F$, $Z_f \neq \emptyset$ and $\mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_f^{-1}[Z_f])$. As in the proof of Lemma 10.2(4) it follows for $d \in \mathbf{GC}$ with $Z_d \neq \emptyset$ and $K = \mathbf{t}[Z_d]$ that $\mathbf{S}_{\mathbf{K}}^*(K)$, if $d \in F$ or, $0 \notin F$ and $d \notin F$, and $R_K^d(\mathbf{av}_1^{-1}[K])$, if $d \notin F$, but $0 \in F$. Thus, we have that

$$((\exists E' \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_{E'} \wedge (\forall e \in E') (K_e \neq \emptyset \wedge R_K^d(\mathbf{av}_e^{-1}[K_d]))) \vee \mathbf{S}_{\mathbf{K}}^*(K)).$$

With the monotonicity and the idempotency of \Downarrow^* and $\Downarrow^* \vee$ distribution we therefore obtain

$$\begin{aligned} \Downarrow^*((\exists F \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (Z \subseteq \mathbf{II}_F \wedge (\forall f \in F) (Z_f \neq \emptyset \wedge \mathbf{S}_{\mathbf{K}}^*(\mathbf{av}_f^{-1}[Z_f]))) \rightarrow \\ \Downarrow^*(\Downarrow^*((\exists E' \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_{E'} \wedge (\forall e \in E') \\ (K_e \neq \emptyset \wedge R_K^d(\mathbf{av}_e^{-1}[K_e]))) \vee \mathbf{S}_{\mathbf{K}}^*(K))), \end{aligned}$$

of which (11.1) is a direct consequence. \square

By co-induction we now obtain the first inclusion we are looking for.

Proposition 11.2. $\mathbf{S}_{\mathbf{K}}^* \subseteq \mathbf{G}_{\mathbf{K}}^*$.

Let us now start with proving the converse inclusion. Again we need some technical results.

Lemma 11.3. $\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow \mathbf{G}_{\mathbf{K}}^*(-K)$.

Proof. Let $P \stackrel{\text{Def}}{=} \{K \mid \mathbf{G}_{\mathbf{K}}^*(-K)\}$. We prove $P \subseteq \mathbf{G}_{\mathbf{K}}^*$ by strong co-induction. That is, we must show that

$$P(K) \rightarrow (\mathbf{G}^*(\mathbf{min} K) \wedge \mathbf{G}^*(\mathbf{max} K) \wedge (\forall d \in \mathbf{GC}) (K_d \neq \emptyset \rightarrow (P(\mathbf{t}[K_d]) \vee \mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[K_d])))).$$

Assume that $P(K)$. Then $\mathbf{G}_{\mathbf{K}}^*(-K)$ and hence $\mathbf{D}_{\mathbf{K}}^*(-K)$ and $\mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[(-K)_d])$, for $d \in \mathbf{GC}$ with $(-K)_d \neq \emptyset$. Note that $\mathbf{t}(x) = \mathbf{t}(-x)$ and $(-K)_d = -(K_{(-d)})$. Thus, $\mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[K_d])$, for $d \in \mathbf{GC}$ with $K_d \neq \emptyset$. By Lemma 7.4 it follows that $\mathbf{G}^*(\mathbf{max} K)$ and $\mathbf{G}^*(\mathbf{min} K)$. Moreover, as $\mathbf{t}(x) = \mathbf{t}(-x)$ and $(-K)_d = -(K_{(-d)})$, $\mathbf{G}_{\mathbf{K}}^*(\mathbf{t}[K_d])$, for all $d \in \mathbf{GC}$ with $K_d \neq \emptyset$. \square

Lemma 11.4. For $d \in \mathbf{GC}$,

$$\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow K_d \neq \emptyset \rightarrow \mathbf{G}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[K_d]).$$

The statement follows as in case of Lemma 10.6.

Lemma 11.5. Let $K \subseteq \mathbf{II}_1$. Then

$$\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow \mathbf{G}_{\mathbf{K}}^*((\lambda x. 1 - x)[K]).$$

The proof proceeds as in Lemma 10.7 by using Lemma 7.6.

Lemma 11.6. Let $K \in \mathbf{K}$. Then

$$\mathbf{G}_{\mathbf{K}}^*(1/2K) \rightarrow \mathbf{G}_{\mathbf{K}}^*(K).$$

The result follows as in Lemma 10.8 by applying Lemma 7.7.

Lemma 11.7.

$$\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset)).$$

Proof. The proof follows the derivation of Lemma 10.9. Set

$$A(K) \stackrel{\text{Def}}{=} (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset).$$

Then the assertion is

$$\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow \Downarrow^*(A(K)).$$

Let again

$$\begin{aligned} B_0^{\min} &\stackrel{\text{Def}}{=} \mathbf{min} K \neq 0, & B_1^{\min} &\stackrel{\text{Def}}{=} \mathbf{t}(\mathbf{min} K) \neq 0, \\ B_0^{\max} &\stackrel{\text{Def}}{=} \mathbf{max} K \neq 0, & B_1^{\max} &\stackrel{\text{Def}}{=} \mathbf{t}(\mathbf{max} K) \neq 0. \end{aligned}$$

and

$$C_{i,j} \stackrel{\text{Def}}{=} B_i^{\min} \wedge B_j^{\max},$$

for $i, j \in \{0, 1\}$. As we have seen in the proof of Lemma 10.9, it suffices to show that

1. $\Downarrow^*(A(K)) \upharpoonright_{C_{0,0}}$,
2. $\Downarrow^*(A(K)) \upharpoonright_{C_{0,1}}$,
3. $\Downarrow^*(A(K)) \upharpoonright_{C_{1,0}}$,
4. $\Downarrow^*(A(K)) \upharpoonright_{C_{1,1}}$.

Assume that $\mathbf{G}_{\mathbf{K}}^*(K)$ and note for $x \in \{\mathbf{min} K, \mathbf{max} K\}$ that $\mathbf{G}^*(x)$ entails $\mathbf{G}^*(\mathbf{t}(x))$.

From both we obtain that $\Downarrow^*(\mathbf{B}(x)) \upharpoonright_{x \neq 0}$ and $\Downarrow^*(\mathbf{B}(\mathbf{t}(x))) \upharpoonright_{\mathbf{t}(x) \neq 0}$. Because of Rules (\upharpoonright - \wedge), (\upharpoonright -*mon*), and (\upharpoonright -*antimon*) it follows that

$$(\Downarrow^*(\mathbf{B}(x)) \wedge \Downarrow^*(\mathbf{B}(y))) \upharpoonright_{x \neq 0 \wedge y \neq 0},$$

from which we obtain with Rules (\Downarrow - \wedge -*intro*) and (\upharpoonright -*mon*) that

$$\Downarrow^*(\mathbf{B}(x) \wedge \mathbf{B}(y)) \upharpoonright_{x \neq 0 \wedge y \neq 0}. \quad (11.2)$$

As we have seen in the proof of Lemma 10.9,

$$(\mathbf{B}(x) \wedge \mathbf{B}(y)) \rightarrow \Downarrow^*(A(K)),$$

for each choice of x and y . With Rules (\Downarrow -*mon*) and (\Downarrow -*idem*) we thus have that

$$\Downarrow^*(\mathbf{B}(x) \wedge \mathbf{B}(y)) \rightarrow \Downarrow^*(A(K)).$$

Consequently, by (11.2) and Rule (\upharpoonright -*mon*), we obtain that $\Downarrow^*(A(K)) \upharpoonright_{C_{i,j}}$, for $i, j \in \{0, 1\}$. \square

Proposition 11.8. $\mathbf{G}_{\mathbf{K}}^* \subseteq \mathbf{S}_{\mathbf{K}}^*$.

Proof. The statement follows by co-induction. We need to show that

$$\mathbf{G}_{\mathbf{K}}^*(K) \rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}^*(\text{av}_d^{-1}[K_d])))).$$

From Lemmas 11.4 and 11.6 it follows

$$\begin{aligned} \mathbf{G}_{\mathbf{K}}^*(K) &\rightarrow ((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset) \\ &\rightarrow (\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD})) (K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}^*(\text{av}_d^{-1}[K_d])))). \end{aligned}$$

By monotonicity of \Downarrow^* we thus obtain

$$\begin{aligned} \mathbf{G}_{\mathbf{K}}(K) &\rightarrow (\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD}))(K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset))) \\ &\rightarrow \Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD}))(K \subseteq \mathbf{II}_E \wedge (\forall d \in E) (K_d \neq \emptyset \wedge \mathbf{G}_{\mathbf{K}}^*(\mathbf{av}_d^{-1}[K_d]))))), \end{aligned}$$

where, the assumption $\Downarrow^*((\exists E \in \mathbf{P}_{\text{fin}}(\mathbf{SD}))(K \subseteq \mathbf{II}_E \wedge (\forall d \in E) K_d \neq \emptyset))$ can be discharged by Lemma 11.7. \square

As a consequence of Propositions 11.2 and 11.8 we now obtain our central result for the compact sets case.

Theorem 11.9. $\mathbf{S}_{\mathbf{K}}^* = \mathbf{G}_{\mathbf{K}}^*$.

12. CONCLUSION

In this paper the computational power of infinite Gray code has been re-considered and compared with the signed digit representation which is mostly used in applications. Infinite Gray code is a redundancy-free representation of the real numbers, whereas the signed digit representation has a high degree of redundancy: every real number has infinitely many names. Instead of all real numbers only the interval $[-1, 1]$ was considered.

The central aim was to study the relationship between both representations without having to discuss the manipulation of code words directly. To this end, for each of the two kinds of representation, co-inductive characterisations for the spaces under consideration were introduced in a formal logical system as predicates \mathbf{G} and \mathbf{S} , from which the representation can be recovered via a realisability interpretation. Instead of dealing with representations directly, the predicates were compared. Computable translations between the representations can be extracted from the formal proofs. The proofs also guarantee the correctness of the extracted programs.

As was known from earlier studies by Tsuiki [Ts02, TS05], infinite Gray code can be translated into signed digit code in a sequential way; for the converse translation, however, one has to allow the computations to proceed concurrently. In [BT21b], Berger and Tsuiki introduced a modality \Downarrow for concurrency. $\Downarrow(A)$ has no effect on the classical validity of the formula A , but on its realisability interpretation: two concurrent processes try to realise A , in case $\Downarrow(A)$ is realisable, at least one of them will do so. With help of this modality a predicate \mathbf{S}_2 was co-inductively defined, the realisers of which are again streams of signed digits. However, they can be computed concurrently. It was shown that $\mathbf{S} \subseteq \mathbf{G} \subseteq \mathbf{S}_2$.

In the present paper the set of rules coming with the modality \Downarrow was enlarged by two new realisable rules, and several other useful rules were derived. Moreover, the modality was inductively extended to a modality \Downarrow^* of bounded non-determinism, co-inductively leading to predicates \mathbf{G}^* and \mathbf{S}^* . Proof rules for the new modality were derived, and by this way it was shown that $\mathbf{G}^* = \mathbf{S}^*$, thus extending the result in [BT21b].

A powerful proof tool in the proof of the inclusion $\mathbf{S} \subseteq \mathbf{G}$ case was Archimedean induction. Here, a similar rule was presented for the concurrent case.

In [BS16, Sp21] the present authors have given a co-inductive characterisation of the hyperspace of all non-empty compact subsets of a given digit space. Instead of streams of digits, as in the point case, extracted realisers are now finitely branching infinite trees

with nodes being labelled with digits. By doing so, in particular a canonical way of lifting the signed digit representation of the real numbers in $[-1, 1]$ to a representation of the non-empty compact subsets of $[-1, 1]$ is obtained. The representation is very natural: the infinite paths of a tree representing a compact set K correspond to the streams representing the elements of K .

A central aim of the present research was to do analogous investigations for the lifted representations as was done in the point case. The situation turned out very similar to the point case. Predicates $\mathbf{G}_K, \mathbf{S}_K$ and \mathbf{S}_K^* were defined co-inductively and the inclusions $\mathbf{S}_K \subseteq \mathbf{G}_K \subseteq \mathbf{S}_K^*$ shown. Note, however, that for the last inclusion one had to use the stronger modality \Downarrow^* in the definition of a predicate for ‘concurrent’ signed digit representation, whereas in the point case the use of \Downarrow sufficed. A co-inductive predicate \mathbf{G}_K^* for ‘concurrent’ Gray code was introduced as well and $\mathbf{G}_K^* = \mathbf{S}_K^*$ derived.

Moreover, an Archimedean induction rule for non-empty compact subsets was obtained.

A computability-theoretic approach to representing compact sets is carried out in work by Pauly and Tsuiki [PT] who show in particular that $\mathcal{K}(\mathbb{I})$ has a faithful \mathbb{T}^ω -representation $\mathbb{T}^\omega \rightarrow \mathcal{K}(\mathbb{I})$. Here, \mathbb{T} is the partial order $(\{\perp, 0, 1\}, \sqsubseteq)$ with $\perp \sqsubseteq 0, 1$. In this study compact sets are represented as trees as well, but then converted to bottomed sequences in such a way that for finite sets the number of bottoms in the sequence increased by 1 coincides with the cardinality of the set. The exact relationship of this kind of Gray code for $\mathcal{K}(\mathbb{I})$ with the one introduced in the present paper will have to be investigated in future work. Since the constructions given by Pauly and Tsuiki use coding and dove-tailing techniques, which correspond to a direct reference to a fixed operational semantics, it is unclear whether they can be recast in our abstract setting.

ACKNOWLEDGEMENT

This research has been started during the Hausdorff trimester “Types, Sets and Construction” at the Hausdorff Research Institute for Mathematics, Bonn, 2018. The authors are grateful to the organisers of the trimester for having arranged this inspiring meeting and to the Hausdorff Institute for providing such excellent working conditions.

Thanks are due to the referees for their careful reading of the paper. They did a wonderful job: errors in results could be eliminated and the overall presentation of the paper improved.

REFERENCES

- [Be11] U. Berger, From coinductive proofs to exact real arithmetic: theory and applications, *Logical Methods in Computer Science* 7(1) (2011) 1–24, doi: 10.2168/LMCS7(1:8)2011.
- [Be16] U. Berger, Extracting non-deterministic concurrent programs, in J.-M. Talbot, L. Regnier, editors, *25th EACSL Annual Conference on Computer Science Logic (CSL 2016)*, Leibniz International Proceedings in Informatics (LIPIcs), vol. 62, Dagstuhl, Germany, 2016, pages 26:1–26:21; doi.org/10.4230/LIPIcs.CSL.2016.26.
- [Be17] U. Berger. Manuscript. 2017.
- [BH08] U. Berger, T. Hou, Coinduction for exact real number computation, *Theory of Computing Systems* 43 (2008) 394–409, doi: 10.1007.s0022400790176.
- [BMST] U. Berger, K. Miyamoto, H. Schwichtenberg, H. Tsuiki, H. (2016). Logic for Gray-code computation, in D. Probst, P. Schuster, editors, *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, De Gruyter, Berlin, 2016, doi: 10.1515/9781501502620-005.

- [BS16] U. Berger, D. Spreen. A coinductive approach to computing with compact sets, *J. Logic & Analysis* 8(3) (2016) 1–35; doi: 10.4115/jla.2016.8.3.
- [BT21a] U. Berger, H. Tsuiki, Intuitionistic fixed point logic, *Annals Pure Applied Logic* 172(3) (2021), doi.org/10.1016/j.apal.2020.102903.
- [BT21b] U. Berger, H. Tsuiki. Extracting total Amb programs from proofs, in I. Sergey, editors, *Programming Languages and Systems, ESOP 2022*, Lect. Notes Comp. Sci., vol. 13240, Springer-Verlag, Cham, 2022, pages 85–113, doi: 10.1007/978-3-030-99336-8_4.
- [CG06] A. Ciaffaglione, P. Di Gianantonio, A certified, corecursive implementation of exact real numbers, *Theoretical Computer Science* 351 (2006) 39–51; doi: 10.1016/j.tcs.2005.09.061.
- [EH02] A. Edalat, R. Heckmann, Computing with real numbers: I. The LFT approach to real number computation; II. A domain framework for computational geometry, in G. Barthe, P. Dybjer, L. Pinto, J. Saraiva, editors, *Applied Semantics — Lecture Notes from the International Summer School*, Caminha, Portugal, Springer-Verlag, Berlin, 2002, pages 193–267; doi: 10.1007/35404569965.
- [Ed96] A. Edalat, Power domains and iterated function systems, *Information and Computation* 124 (1996) 182–197; doi.org/10.1006/inco.1996.0014.
- [ES98] A. Edalat, P. Sünderhauf, A domain-theoretic approach to real number computation, *Theoretical Computer Science* 210 (1998) 73–98, doi: 10.1016/S03043975(98)000978.
- [GHKLMs03] G. Gierz, K. H. Hofmann, K. Keimel, J. D. Lawson, M. Mislove, and D. S. Scott. *Continuous Lattices and Domains*, Cambridge University Press, Cambridge, 2003.
- [Let02] P. Letouzey, A New Extraction for Coq. in *TYPES 2002*, Lect. Notes Comp. Sci., vol. 2646, Springer-Verlag, Berlin, 2011, pages 200–219; doi.org/10.1007/3-540-39185-1_12.
- [MC63] McCarthy, J.: A basis for a mathematical theory of computation. In: Braffort, P., Hirschberg, D. (eds.) *Computer Programming and Formal Systems*, Studies in Logic and the Foundations of Mathematics, vol. 35, pp. 33 – 70. Elsevier (1963).
- [ME07] J. R. Marcial-Romero, M. Hötzel Escardó, Semantics of a sequential language for exact real number computation, *Theoretical Computer Science* 379(12) (2007) 120–141, doi: 10.1016/j.tcs.2007.01.021.
- [Min11] U. Berger, K. Miyamoto, H. Schwichtenberg, M. Seisenberger, Minlog - A Tool for Program Extraction for Supporting Algebra and Coalgebra, in *Proc. of CALCO-Tools*, Lect. Notes Comp. Sci., vol. 6859, Springer-Verlag, Berlin, 2011, pages 393–399; doi.org/10.1007/978-3-642-22944-2_29.
- [PT] A. Pauly, H. Tsuiki. Computable dyadic subbases and T^ω -representations of compact sets. <https://arxiv.org/abs/1604.00258>.
- [Pl77] G. D. Plotkin, LCF considered as a programming language, *Theoretical Computer Science* 5 (1977) 223–255.
- [Sc79] D. S. Scott, Identity and existence in intuitionistic logic, in M. Fourman et al., editors, *Applications of sheaves, Proc. Res. Symp. Durham 1977*, Lect. Notes Math., vol. 753, Springer-Verlag, Berlin, 1979, pages 660–669.
- [Sp21] D. Spreen, Computing with continuous objects: a uniform co-inductive approach, *Mathematical Structures in Computer Science* 31(2) (2021) 144–192, doi: 10.1017/S0960129521000116.
- [Ts02] H. Tsuiki, Real number computation through Gray code embedding, *Theoretical Computer Science* 284(2) (2002) 467–485; doi.org/10.1016/S0304-3975(01)00104-9.
- [TS05] H. Tsuiki, K. Sugihara, Streams with a bottom in functional languages, in M. Sagiv, editor, *ESOP 2005*, Lec. Notes Comput. Sci., vol. 3444, Springer-Verlag, Berlin, 2005, pages 201–216; doi.org/10.1007/978-3-540-31987-0_15.
- [We00] K. Weihrauch, *Computable Analysis*, Springer Verlag, Berlin, 2000, doi: 10.1007/9783642569999.